(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－85015

(43)公開日　平成11年(1999)３月30日

(51)Int.Cl.⁶		識別記号	FI		
G09C	1/00	630	G09C	1/00	630Z
H04L	9/08		H04L	9/00	601Z

審査請求　未請求　請求項の数34　ＯＬ　（全 30 頁）

(21)出願番号　特願平10－191899

(22)出願日　平成10年(1998)７月７日

(31)優先権主張番号　特願平9－181627

(32)優先日　平９(1997)７月７日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(74)代理人　弁理士　大菅　義之　(外１名)

最終頁に続く

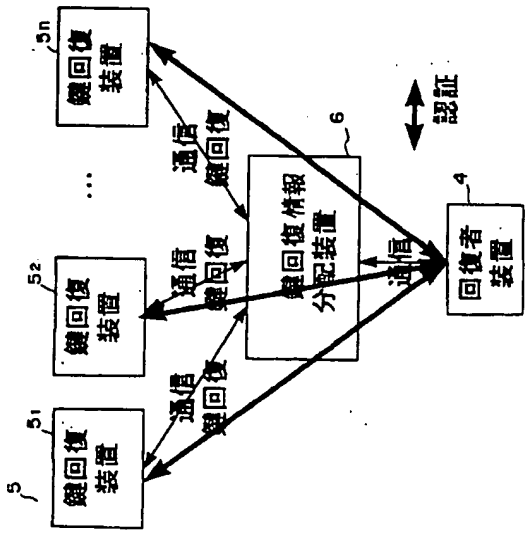
(54)【発明の名称】　鍵回復システム

(57)【要約】

【課題】　回復者装置と鍵回復装置の間に設けられ、鍵情報分配装置が認証データの回復者装置にかわってデータ鍵を回復するとともにその負荷を軽減する。

【解決手段】　データをデータ鍵で暗号化し、鍵回復情報とともに保管しておき、鍵を紛失したとき、暗号の回復者装置が鍵回復情報を鍵回復情報分配装置を介して鍵回復装置に分配して鍵情報を回復し、鍵回復装置と回復者装置との間で直接認証を行ってから鍵情報を回復者装置に転送し、回復者装置でデータ鍵を回復する。

本発明の原理にかかる
鍵回復システムの原理を示すブロック図



1

【特許請求の範囲】

【請求項１】　暗号化データとともに、暗号化したデータ鍵を含む鍵回復情報を格納し、暗号化データに添付してある鍵回復情報からデータ鍵を取り出し、暗号化データを復号する鍵回復システムにおいて、

鍵の回復を要求する回復者装置、回復要求に応じて対応する鍵回復装置へ通信路を提供する鍵回復情報分配装置、鍵回復情報からデータ鍵、あるいはその一部を復号して取り出し、回復者の認証を回復者装置と直接行う少なくとも１つの鍵回復装置からなることを特徴とする鍵回復システム。

【請求項２】　前記認証は回復者装置のパスワードの一致を鍵回復装置で判断することにより行われることを特徴とする請求項１記載の鍵回復システム。

【請求項３】　前記認証は回復者装置と鍵回復装置との間で共有されたセッション鍵で暗号化されたメッセージを用いて行うことを特徴とする請求項１記載の鍵回復システム。

【請求項４】　前記鍵回復情報分配装置は、鍵回復装置の認証要求および回復者装置の認証応答を中継する認証情報中継部を有することを特徴とする請求項１記載の鍵回復システム。

【請求項５】　前記データ鍵は、鍵回復装置から取得した公開鍵で暗号化されて鍵回復情報として記憶されるとともに、前記データ鍵は、前記回復者装置の公開鍵で暗号化されて回復者装置に保管され、通常時は、データ鍵で暗号化データを復号するが、該回復者装置の秘密鍵がない場合、前記鍵回復情報を用いてデータ鍵を復号することを特徴とする請求項１記載の鍵回復システム。

【請求項６】　鍵回復情報はさらに鍵回復条件を含み、回復要求を鍵回復情報分配装置を経由して鍵回復装置に伝え、回復条件に従った回復者の認証を鍵回復情報分配装置を経由しながら回復者装置と鍵回復装置が直接行い、認証が有効であった場合は、鍵回復装置が鍵回復分配装置を経由しながら鍵情報を回復者装置に送り、回復者装置が鍵情報をもとに鍵を回復することを特徴とする請求項１記載の鍵回復システム。

【請求項７】　鍵回復装置から回復者装置に送られる鍵情報は鍵回復装置と回復者装置との間の共通のセッション鍵で暗号化されていることを特徴とする請求項５記載の鍵回復システム。

【請求項８】　データ鍵に基づくデータの回復を回復者装置で行うことを特徴とする請求項５記載の鍵回復システム。

【請求項９】　認証を回復情報分配装置を介さずに回復者装置と鍵回復装置との間の直接接続路を介して行うことを特徴とする請求項５記載の鍵回復システム。

【請求項１０】　データ鍵に基づくデータの回復を回復者装置が行うことを特徴とする請求項９記載の鍵回復システム。

2

【請求項１１】　鍵回復情報はさらに鍵回復条件を含み、回復要求を鍵回復情報分配装置を経由して鍵回復装置に伝え、回復条件に従った回復者の認証を鍵回復情報分配装置を経由しながら回復者装置と鍵回復装置が直接行い、認証が有効であった場合は、鍵回復装置から鍵情報を鍵回復情報分配装置が得て、鍵回復情報分配装置が鍵情報を元に鍵を回復し、その鍵を回復者装置に伝えることを特徴とした請求項１記載の鍵回復システム。

【請求項１２】　データ鍵に基づくデータの回復を鍵回復情報分配装置で行うことを特徴とする請求項１１記載の鍵回復システム。

【請求項１３】　認証を回復者装置と鍵回復装置との間で鍵回復情報分配装置を介さずに直接接続路を介して行うことを特徴とする鍵回復情報を特徴とする請求項１１記載の鍵回復システム。

【請求項１４】　データ鍵にもとづくデータの回復を鍵回復情報分配装置において行うことを特徴とする請求項１３記載の鍵回復システム。

【請求項１５】　鍵回復情報は更に鍵回復装置のＩＤからなることを特徴とする請求項１記載の鍵回復システム。

【請求項１６】　前記鍵回復情報は各鍵回復装置に対して、並列方式に権限分散されることを特徴とする請求項１記載の鍵回復システム。

【請求項１７】　前記鍵回復情報は、各鍵回復装置に対して、順序方式により権限分散されて構成されたことを特徴とする請求項１記載の鍵回復装置の鍵回復システム。

【請求項１８】　前記回復情報分配装置は鍵回復装置のＩＤと、各鍵回復装置の名前、そのアクセスアドレス、通信プロトコルの対応テーブルをデータベースとして有することを特徴とする請求項１記載の鍵回復システム。

【請求項１９】　暗号文に鍵回復情報を添付して記憶し、鍵回復要求があった場合にはその鍵回復要求を送信し、認証要求を受信した場合に鍵回復者が認証情報を入力して認証返答情報を送信し、鍵情報を受信した場合に鍵を回復する回復者装置と、

鍵回復情報を前記回復者装置から受信した場合にデータベースから鍵回復情報に基づいて鍵回復装置のアクセス情報を取得すると共に鍵回復情報を鍵回復装置へ分配し、認証要求を受信した場合には、前記回復者装置に該認証要求を送信し、この認証要求に応じて、回復者装置から認証応答を受信した場合にこの認証応答を鍵回復装置に送信し、鍵情報を受信した場合にこれを回復者装置に送信する鍵回復情報分配装置と、

鍵回復情報を受信した場合に鍵回復情報から鍵情報を得、この鍵情報を用いて回復条件を復号し、その回復条件に基づく認証要求を回復者装置に前記鍵回復情報分配装置を介して送り、認証応答を回復者装置から受信した場合には認証応答の検証を行うことにより回復者装置と

直接認証を行い、この認証が正しかった場合には鍵情報を鍵回復情報分配装置を介して回復者装置に転送する少なくとも１つの鍵回復装置とからなることを特徴とする鍵回復システム。

【請求項２０】　鍵回復情報を回復者装置から鍵回復情報分配装置を介して少なくとも１つの鍵回復装置に分配して鍵を回復する鍵回復システムに用いられ、暗号文を鍵回復情報を添付して記憶し、鍵回復要求があった場合にはその鍵回復要求を送信することにより認証を鍵回復装置と直接行い、認証要求を受信した場合に鍵回復者が認証情報を入力して認証返答情報を送信し、鍵情報を受信した場合に鍵を回復することを特徴とする回復者装置。

【請求項２１】　鍵回復情報を回復者装置から鍵回復情報分配装置を介して少なくとも１つの鍵回復装置に分配して鍵を回復する鍵回復システムに用いられ、鍵回復情報を回復者装置から受信した場合にデータベースから鍵回復情報に基づいて鍵回復装置のアクセス情報を取得し、認証要求を受信した場合には、回復者装置に該認証要求を送信し、この認証要求に応じて、回復者装置から認証応答を受信した場合にこの認証応答を回復装置に送信し、鍵情報を受信した場合にこれを回復者装置に送信することを特徴とする鍵回復情報分配装置。

【請求項２２】　鍵回復情報を回復者装置から鍵回復情報分配装置を介して少なくとも１つの鍵回復装置に分配して鍵を回復する鍵回復システムに用いられ、鍵回復情報を受信した場合に鍵回復情報から鍵を得、この鍵を用いて回復条件を復号し、その回復条件に基づく認証要求を鍵回復者装置に送り、認証応答を鍵回復者装置から受信した場合には認証応答の検証を行い、この検証が正しかった場合には鍵情報を回復者装置に転送することを特徴とする鍵回復装置。

【請求項２３】　データ鍵の回復を要求する回復者装置と、
鍵回復要求に応じて対応する鍵回復装置に通信路を提供する鍵回復情報分配装置と、
鍵回復情報からデータ鍵あるいはデータ鍵情報を復号して取り出す少なくとも１つの鍵回復装置と、
前記回復者装置から前記鍵回復情報分配装置を介して各鍵回復装置に鍵回復情報を送信して、データ鍵と回復条件を回復する手段と、
該回復条件に従って前記回復者装置と前記鍵回復装置が直接認証を行う手段と、
前記認証が成立した場合、前記鍵回復装置で回復されたデータ鍵あるいはデータ鍵情報を回復者装置に送信する手段とからなる鍵回復システム。

【請求項２４】　暗号化データとともに、暗号化したデータ鍵と回復条件とからなる鍵回復情報を格納し、前記データ鍵を復号する鍵がないとき、データ鍵の回復を要求する回復者ステップ、回復要求に応じて対応する鍵回復ステップへ通信路を提供する鍵回復情報分配ステップ、鍵回復情報からデータ鍵、あるいはその一部を復号して取り出し、回復者の認証を前記鍵回復者ステップと前記鍵回復ステップとで直接行う少なくとも１つの鍵回復ステップからなることを特徴とする鍵回復方法。

【請求項２５】　回復要求を鍵回復情報分配ステップを経由して鍵回復ステップに伝え、回復条件に従った回復者の認証を鍵回復情報分配ステップを経由しながら回復者ステップと鍵回復ステップが直接行い、認証が有効であった場合は、鍵回復装置が鍵回復情報分配ステップを経由しながら鍵情報を回復者ステップに送り、回復者ステップが鍵情報をもとに鍵を回復することを特徴とする請求項２４記載の鍵回復方法。

【請求項２６】　回復要求を鍵回復情報分配ステップを経由して鍵回復ステップに伝え、回復条件に従った回復者の認証を鍵回復情報分配ステップを経由しながら回復者ステップと鍵回復ステップが直接行い、認証が有効であった場合は、鍵回復ステップから鍵情報を鍵回復情報分配ステップが得て、鍵回復情報分配ステップが鍵情報を元に鍵を回復し、その鍵を回復者ステップに伝えることを特徴とした請求項２４記載の鍵回復方法。

【請求項２７】　暗号文を鍵回復情報を添付して記憶し、鍵回復要求があった場合にはその鍵回復要求を送信し、認証要求を受信した場合に鍵回復者が認証情報を入力して認証返答情報を送信し、鍵情報を受信した場合に鍵を回復する回復者ステップと、
鍵回復情報を前記回復者ステップから受信した場合にデータベースから鍵回復情報に基づいて鍵回復ステップのアクセス情報を取得すると共に、鍵回復情報を鍵回復ステップに分配し、鍵情報を受信した場合にこれを回復者ステップに送信する鍵回復情報分配ステップと、
鍵回復情報を受信した場合に鍵情報を得、この鍵情報を用いて認証要求を回復者ステップに前記鍵回復情報分配ステップを介して送り、認証応答を回復者ステップから受信した場合には認証応答の検証を行い、この検証が正しかった場合には鍵情報を鍵回復情報分配ステップを介して回復者ステップに転送する鍵回復ステップとからなることを特徴とする鍵回復方法。

【請求項２８】鍵の回復を要求する鍵回復者装置と、
鍵回復要求に応じて対応する回復装置に通信路を提供する分配装置と、
鍵回復情報からデータ鍵情報の一部を復号して取り出す少なくとも１つの鍵回復装置を用いて、データ鍵を復号する鍵がない場合にデータ鍵を回復する方法において、
鍵回復者装置から鍵情報分配装置を介して各鍵回復装置に鍵回復情報を送信して、データ鍵と回復条件を回復するステップと、
該回復条件に従って前記回復者装置と前記鍵回復装置が直接認証を行うステップと、
前記認証が成立した場合、前記鍵回復装置で回復された

鍵を回復者装置に送信するステップとからなることを特徴とする鍵回復方法。

【請求項２９】　暗号化データとともに、公開鍵で暗号化したデータ鍵と回復条件とからなる鍵回復情報を格納し、通常時は、そのデータ鍵で暗号化データを回復するが、データ鍵なしで復号するために、鍵の回復を要求する回復者機能、回復要求に応じて対応する鍵回復機能へ通信路を提供する鍵回復情報分配機能、鍵回復情報からデータ鍵、あるいはその一部を復号して取り出し、回復者の認証を前記鍵回復者機能と前記鍵回復機能とで直接行う少なくとも１つの鍵回復機能を計算機に行わせることを特徴とする計算機読み出し可能な記録媒体。

【請求項３０】　暗号文を鍵回復情報を添付して記憶し、鍵回復要求があった場合にはその鍵回復要求を送信し、認証要求を受信した場合に鍵回復者が認証情報を入力して認証返答情報を送信し、鍵情報を受信した場合に鍵を回復する回復者機能と、

鍵回復情報を前記回復者機能から受信した場合にデータベースから鍵回復情報に基づいて鍵回復機能のアクセス情報を取得すると共に鍵回復情報を鍵回復装置に分配し、認証要求を受信した場合には、前記回復者機能に該認証要求を送信し、この認証要求に応じて、回復者機能から認証応答を受信した場合にこの認証応答を回復者機能に送信し、鍵情報を受信した場合にこれを回復者機能に送信する鍵回復情報分配機能と、

鍵回復情報を受信した場合に鍵回復情報を得、この鍵情報を用いて認証要求を鍵回復者機能に前記鍵回復情報分配機能を介して送り、認証応答を回復者機能から受信した場合には認証応答の検証を行うことにより回復者機能と直接認証を行い、この検証が正しかった場合には鍵情報を鍵回復情報分配機能を介して回復者機能に転送する鍵回復機能とを計算機に行わせることを特徴とする計算機読み出し可能な記録媒体。

【請求項３１】鍵の回復を要求する回復者機能と、

鍵回復要求に応じて対応する鍵回復機能に通信路を提供する鍵回復情報分配機能と、

鍵回復情報からデータ鍵情報の一部を復号して取り出す少なくとも１つの鍵回復機能、

前記鍵回復者機能から前記鍵回復情報分配機能を介して各鍵回復機能に鍵回復情報を送信して、データ鍵と回復条件を回復する機能と、

該回復条件に従って前記回復者機能と前記鍵回復機能が直接認証を行う機能と、

前記認証が成立した場合、前記鍵回復機能で回復された鍵を回復者機能に送信する機能とを計算機に行わせることを特徴とする計算機読み出し可能な記録媒体。

【請求項３２】　暗号文を鍵回復情報を添付して記憶し、鍵回復要求があった場合にはその鍵回復要求を送信することにより認証を鍵回復機能と直接行い、認証要求を受信した場合に鍵回復者が認証情報を入力して認証返答情報を送信し、鍵情報を受信した場合に鍵を回復する機能を計算機に行わせることを特徴とする計算機読み出し可能な記録媒体。

【請求項３３】　鍵回復情報を回復者機能から受信した場合にデータベースから鍵回復情報に基づいて鍵回復機能のアクセス情報を取得し、認証要求を受信した場合には、回復者機能に該認証要求を送信し、この認証要求に応じて、回復者機能から認証応答を受信した場合にこの認証応答を鍵回復機能に送信することにより認証を回復者機能と鍵回復機能との間で直接行い、鍵情報を受信した場合にこれを回復者機能に送信することにより鍵回復情報分配機能を計算機に行わせることを特徴とする計算機読み出し可能な記録媒体。

【請求項３４】　鍵回復情報を受信した場合に鍵回復情報から鍵を得、この鍵を用いて回復条件を復号し、その回復条件に基づく認証要求を回復者機能に送り、認証応答を回復者機能から受信した場合には認証応答の検証を行うことにより認証を回復者機能と鍵回復機能との間で直接行い、この検証が正しかった場合には鍵情報を回復者機能に転送する鍵回復機能計算機に行わせることを特徴とする計算機読み出し可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、例えばデータを鍵で暗号化して暗号文として保管する場合、ユーザの担当者が不在であったり、ユーザの秘密鍵が紛失した時などの緊急時に、暗号文の鍵を回復する鍵回復システムに関する。

【０００２】

【従来の技術】鍵回復システムを実現するためには、予め各ユーザの鍵を預けておく方法と、システムの鍵でデータの鍵を暗号化しておく方式がある。本発明は、後者の方式による鍵回復システムである。

【０００３】各ユーザは、データを暗号化する場合に、暗号化したデータとともに、データを暗号化した鍵（以下、データ鍵と呼ぶ）を、予め入手したシステム鍵（以下、公開鍵と呼ぶ）で暗号化し、回復条件とともに鍵回復情報として格納する。

【０００４】上記公開鍵は、少なくとも１つの鍵回復装置（鍵回復センタともいう）から入手する。ユーザ（回復者装置）が秘密鍵を持っている場合は、データ鍵を自分の公開鍵で暗号化したものを秘密鍵で復号してデータ鍵で暗号化データを復号する。ユーザが秘密鍵を紛失した場合、あるいは緊急に第３者がこの暗号化データを復号する必要がある場合には、データ鍵を鍵回復装置から回復するために暗号化データに添付してある鍵回復情報を取り出し、鍵回復装置に送付する。

【０００５】鍵回復装置は、鍵回復情報を参照し、回復者が回復権限を有するか確認し、ある場合は、鍵回復情報からデータ鍵を復元し、回復者に出力する。従来の鍵

回復システムにおいては、鍵回復装置は、秘密鍵を有しているため、その公開鍵で暗号化されたデータ鍵を含む鍵回復情報を添付しているすべての暗号文を回復することができてしまう。これを避けるため鍵回復装置の回復能力を分散させる必要がある。このため、鍵回復装置を複数用意し、複数の鍵回復装置の公開鍵（Ｐ１，Ｐ２，・・・）から鍵回復情報を作成し、回復時には全ての鍵回復装置の合意Ｋ１＋Ｋ２＋・・・が得られなければ鍵を回復できないようにする方法が一般的にとられている。

【０００６】図２２は、従来例として、ＩＢＭのＳＫＲ（Secure Key Recovery)方式を示す。図２２に見られるように鍵回復サービスプロバイダ１を設け、回復者装置２の認証は鍵回復サービスプロバイダ１が行い、その認証が正しければ、鍵回復サービスプロバイダ１が鍵回復情報を複数の鍵回復装置３に送信し、各鍵回復装置３が鍵情報を回復し、その鍵情報から鍵回復サービスプロバイダ１を経由して回復者装置２に鍵を返していた。

【０００７】

【発明が解決しようとする課題】図２２の従来の方式では、鍵回復サービスプロバイダ１と回復者の間の認証をもとにデータ鍵を回復していたため、暗号文作成者が鍵回復装置毎に回復条件を指定していた場合、鍵回復サービスプロバイダ１は、鍵回復装置に応じた認証処理に対応できない場合があり、オーバヘッドが大きくなったり、場合によっては、鍵回復ができない場合もありえた。

【０００８】鍵回復サービスプロバイダ１が回復者の認証をあたかも行ったかのように不正を働いた場合には、全ての暗号文を鍵回復サービスプロバイダ１に回復されてしまう問題が生じる。

【０００９】本発明は、回復者装置が全ての鍵回復装置と直接通信しないにもかかわらず、回復者装置と鍵回復装置が直接回復者の認証を行い、その認証を元に回復者装置が最終的に鍵が得られる鍵回復システムを提供することを目的とする。

【００１０】

【課題を解決するための手段】上記問題点を解決するために、図２２の鍵回復サービスプロバイダの代わりに鍵回復情報分配装置を設ける。鍵回復情報分配装置は、関係する鍵回復装置の全情報を管理し、回復者装置の要求にしたがって回復者装置と鍵回復装置の通信を可能にする。ただし、回復者装置の認証は行わない。回復者装置の認証は、鍵回復装置と回復者装置間で直接行う。この場合、鍵回復情報分配装置は、鍵回復装置と回復装置との通信を提供する。そして、その認証を元に回復者装置が最終的に鍵が得られる鍵回復システムを提供する。すなわち、鍵回復情報分配装置は、回復者装置と鍵回復装置の通信を中継するが、回復者装置の認証は行わず、回復者装置の認証は回復者装置のパスワードの一致の判断を鍵回復装置で行うことにより実行される。

【００１１】請求項１記載の発明によれば、暗号化データとともに、公開鍵で暗号化したデータ鍵を含む鍵回復情報を格納し、通常時は、そのデータ鍵で暗号化データを回復するが、データ鍵を復号する秘密鍵がない場合に、暗号化データに添付してある鍵回復情報からデータ鍵を取り出し、暗号化データを復号することのできる鍵回復システムにおいて、鍵の回復を要求する回復者装置、回復要求に応じて対応する鍵回復装置へ通信路を提供する鍵回復情報分配装置、鍵回復情報からデータ鍵、あるいはその一部を復号して取り出し、回復者の認証を回復者装置と直接行う少なくとも１つの鍵回復装置からなることを特徴とする鍵回復システムである。

【００１２】請求項１９記載の発明によれば、暗号文を鍵回復情報を添付して記憶し、鍵回復要求があった場合にはその鍵回復要求を送信し、認証要求を受信した場合に鍵回復者が認証情報を入力して認証返答情報を送信し、鍵情報を受信した場合に鍵を回復する回復者装置と、鍵回復情報を前記回復者装置から受信した場合にデータベースから鍵回復情報に基づいて鍵回復装置のアクセス情報を取得し、認証要求を受信した場合には、前記回復者装置に該認証要求を送信し、この認証要求に応じて、回復者装置から認証応答を受信した場合にこの認証応答を鍵回復装置に送信し、鍵情報を受信した場合にこれを回復者装置に送信する鍵回復情報分配装置と、鍵回復情報を受信した場合に鍵回復情報から鍵情報を得、この鍵情報を用いて認証要求を鍵回復者装置に前記鍵回復情報分配装置を介して送り、認証応答を鍵回復者装置から受信した場合には認証応答の検証を行い、この検証が新しかった場合には鍵情報を鍵回復情報分配装置を介して回復者装置に転送する鍵回復装置とからなる鍵回復システムを提供する。

【００１３】請求項２３の発明によれば鍵の回復を要求する回復者装置と、鍵回復要求に応じて対応する鍵回復装置に通信路を提供する鍵回復情報分配装置と、鍵回復情報からデータ鍵情報の一部を復号して取り出す少なくとも１つの鍵回復装置と、前記鍵回復者装置から前記鍵回復情報分配装置を介して各鍵回復装置に鍵回復情報を送信して、データ鍵と回復条件を回復する手段と、該回復条件に従って前記回復者装置と前記鍵回復装置が直接認証を行う手段と、前記認証が成立した場合、前記鍵回復装置で回復された鍵を回復者装置に送信する手段とからなる鍵回復システムを提供する。

【００１４】請求項２８記載の発明によれば、鍵の回復を要求する回復者装置と、鍵回復要求に応じて対応する鍵回復装置に通信路を提供する分配装置と、鍵回復情報からデータ鍵情報の一部を復号して取り出す少なくとも１つの鍵回復装置を用いて、データ鍵を復号する鍵がない場合にデータ鍵を回復する方法において、鍵回復者装置から鍵情報分配装置を介して各鍵回復装置に鍵回復情

報を送信して、データ鍵と回復条件を回復するステップと、該回復条件に従って前記回復者装置と前記鍵回復装置が直接認証を行うステップと、前記認証が成立した場合、前記鍵回復装置で回復された鍵を回復者装置に送信するステップとからなることを特徴とする鍵回復方法を提供する。

【００１５】請求項２９記載の発明によれば、暗号化データとともに、公開鍵で暗号化したデータ鍵と回復条件とからなる鍵回復情報を格納し、通常時は、そのデータ鍵で暗号化データを回復するが、データ鍵なしで復号するために、鍵の回復を要求する回復者機能、回復要求に応じて対応する鍵回復機能へ通信路を提供する鍵回復情報分配機能、鍵回復情報からデータ鍵、あるいはその一部を復号して取り出し、回復者の認証を前記回復者機能と前記鍵回復機能とで直接行う少なくとも１つの鍵回復機能を計算機に行わせることを特徴とする計算機読み出し可能な記録媒体を提供する。

【００１６】

【発明の実施の形態】図１は、本発明の原理説明図である。図中、回復者装置４は、回復者が回復する暗号文を指定し、直接、鍵回復装置５から要求される認証条件にそった処理を行い、その認証が正しい場合には、鍵を得るものである。

【００１７】回復情報分配装置６は、回復者装置４からの回復要求を受け、鍵回復情報に指定された鍵回復装置５と通信し、鍵回復装置５から要求された回復者への認証要求情報を回復者装置に中継し、鍵回復装置５が回復した鍵情報を回復者装置４に中継するものである。鍵回復装置５は、鍵回復情報分配装置６からの回復要求を受け取り、鍵回復情報分配装置に中継されながら回復者装置４と直接認証情報をやりとりし、その認証が有効であれば、鍵情報を回復するものである。

【００１８】まず、たとえば遺言人である暗号作成者が、データ鍵で暗号化された遺言を鍵回復情報とともに回復者装置４に記録する。その暗号文を復号するべき遺言人が秘密鍵を紛失したり、あるいはその遺言書を読む権利のある人が緊急に遺言書を復号する必要があったとする。

【００１９】回復者装置４から回復者装置４のＩＤ、公開鍵Ｐ、データ鍵Ｋ、回復条件ＲＣからなる鍵回復情報ＩＤ，Ｐ（Ｋ），Ｋ（ＲＣ）を、鍵回復情報分配装置を介して鍵回復装置５のＩＤを用いてその鍵回復装置５に送り、鍵回復装置５では公開鍵Ｐに対する秘密鍵Ｓを使用してデータ鍵Ｋを復号しそのＫを基に回復条件であるＲＣを復元する。ＲＣとしては鍵回復者のパスワードやＩＤ、テキストデータ等が考えられる。そしてＲＣがパスワードの場合はそのパスワードを用いて鍵回復装置５は回復者装置４に認証要求を行う。回復者装置４はその認証要求に応じて、例えば回復者のパスワードを入力する。そして、鍵回復者のパスワードを鍵回復装置５に送り、鍵回復条件検証部にある鍵回復者のパスワードと比較し、一致すれば回復者装置と鍵回復装置５とが直接の認証がとれたことになる。その後、鍵回復装置５は鍵情報を回復者装置４に送信する。鍵回復装置５はデータ鍵Ｋを使って暗号文を復号する。

【００２０】本発明では鍵回復装置５から認証応答があった時点で、例えば回復条件であるパスワードが回復者装置４から入力されたものと鍵回復装置５に記憶されたものが一致した事を見る。これにより回復者装置４が直接、鍵回復装置５と認証を行うので、鍵回復情報分配装置が回復者に成り代わって不正に鍵回復の認証を行うことができない。

【００２１】さらに本発明では、鍵回復分散機能を持つことで、回復者装置４の鍵回復装置５に関する情報の管理を削減し、さらに、鍵回復装置５と直接認証することにより様々な認証条件に対応可能となるとともに、鍵回復情報分配装置がかかる様々な認証条件に対応しきれないという問題も生じない。

【００２２】図２は、本発明の一実施例構成図である。本発明の鍵回復システム１０は、回復者装置１１、鍵回復情報分配装置１２、鍵回復装置１３からなる。

【００２３】回復者装置１１は、鍵回復要求部１１ａ、認証応答部１１ｂ、鍵回復部１１ｃ、暗号処理部１１ｄ、制御部１１ｅ、通信部１１ｆからなる。鍵回復情報取得部１１ｇは鍵回復情報ＩＤ，Ｐ（Ｋ）Ｋ（ＲＣ）を取得する。ＩＤは鍵回復装置ＩＤ、Ｐは鍵回復装置から入手した公開鍵、ＲＣは各鍵回復装置の回復条件である。さらに、データ（平文）はデータ鍵Ｋで暗号化され、そのデータ鍵Ｋは、回復者装置１１の公開鍵で暗号化され、暗号文とされている。そして、暗号文に鍵回復情報が添付されて、回復者装置に保管しておく。

【００２４】鍵回復情報分配装置１２は、鍵回復情報解析部１２ａ、鍵回復装置情報取得部１２ｂ、認証情報中継装置１２ｃ、暗号処理部１２ｄ、制御部１２ｅ、通信部１２ｆからなる。

【００２５】鍵回復装置１３は、鍵情報取得部１３ａ、回復条件検証部１３ｂ、暗号処理部１３ｃ、制御部１３ｄ、通信部１３ｅからなる。図３は、図２の実施例における回復者装置の動作を示すフローチャートである。通常は回復者装置は自分の秘密鍵で自分の公開鍵で暗号化されたデータ鍵を復号して、このデータ鍵で暗号文を復号する。しかし、鍵回復者が自分の秘密鍵を紛失し、データ鍵を復号できず、したがってデータ鍵を回復する必要が生じた場合、すなわち鍵回復要求が回復者装置から発生した場合には、その処理を開始する時点で、まず解読すべき暗号文を指定する（ステップＳ１，Ｓ２）。鍵回復要求部１１ａにおいて鍵回復情報ＩＤ，Ｐ（Ｋ），Ｋ（ＲＣ）を取得し（ステップＳ３）、制御部１１ｅにおいて鍵回復要求メッセージを作成し（ステップＳ４）、通信部１１ｆにおいて鍵回復要求メッセージを鍵

回復情報分配装置に送信する（ステップS5）。すなわち、鍵回復要求者が自分の秘密鍵を紛失した場合には、鍵回復要求を鍵回復情報分配装置12に送信するものである。

【0026】次に、鍵回復要求ではない場合であって、認証要求である場合は（ステップS6）、認証応答部11bにおいて、認証手段を例えばパスワード、ID：テキストデータ等の中から例えばパスワードがあると認識する（ステップS7）。そして、パスワード入力を鍵回復者に促す（ステップS8）。鍵回復者がパスワードを入力し認証応答部11bがパスワードを含んだパスワード返答メッセージを作成し（ステップS9，10）、通信部11fにおいてパスワード返答メッセージを鍵回復情報分配装置12に送信する（ステップS11）。

【0027】次に、認証要求ではなかった場合には鍵情報かを判断し（ステップS12）、鍵情報である場合には、制御部11fは鍵情報を鍵回復部11cに送る（ステップS13）。鍵情報とは、並列方式の場合、各鍵回復装置から送られてきた鍵、K1，K2，K3，．．．Knである。次に、これら鍵情報K1，K2，K3，．．．Knからそれらの排他的論理和をとって鍵Kを回復する（ステップS14）。

【0028】なお、今回の実施例は排他的論理和で鍵を合成するが、閾値法など他の鍵分散方式を用いてもよい。次に鍵Kを制御部に送り（ステップS15）、制御部11eは鍵は回復した旨を回復者装置11に伝える（ステップS16）。鍵情報でもなかった場合には、エラー処理を行う（ステップS17）。

【0029】図4は、図2の実施例における鍵回復情報分配装置の動作を示すフローチャートである。先ず、暗号文が鍵回復者から送られてきた場合、これが鍵回復情報ID，P（K），K（RC）であった場合には（ステップS21）、制御部12eを通して鍵回復情報が鍵回復情報解析部12aに送られる（ステップS22）。鍵回復情報解析部12aは個々の鍵回復情報を取り出す（ステップS23）。

【0030】次に、鍵回復情報は制御部12eを通して鍵回復情報取得部12bに送られる（ステップS24）。鍵回復情報取得部12bは鍵回復情報から鍵回復装置13のIDを取得する（ステップS25）。鍵回復情報取得部12bは図10に示す鍵回復装置データベースから鍵回復装置のIDを使ってアクセス方法を取得する（ステップS26）。

【0031】通信部12fはアクセス方法に従って、鍵回復情報を鍵回復装置13に送信する（ステップS27）。次に、鍵回復装置からの認証要求を受信したと判断した場合の動作はステップS28～S31に示す。すなわち、認証要求メッセージを認証情報中継部12cに送る。認証情報中継部12cは認証要求メッセージを通信部12fに送る。認証要求メッセージを鍵回復者装置11に送る。

【0032】次に鍵回復情報分配装置12が鍵回復者装置11から認証応答を受信したと判断した場合の動作はステップS32～S35に示す。すなわち、、認証応答メッセージを認証情報中継部12cに送る。認証情報中継部12cは認証応答メッセージを通信部12fに送る。通信部12fは認証応答メッセージを鍵回復装置13に送る。

【0033】さらに鍵回復情報分配装置12が鍵回復装置11から鍵情報（K1，K2，K3，・・・Kn）を受信したと判断した場合の動作をステップS36～S40に示す。すなわち、、鍵情報を制御部12eが記憶する。次の鍵回復情報が別の鍵回復装置用に送られてきているか否かを判断し、YESの場合には、その鍵回復情報を制御部12eに送り前述の鍵回復情報を受信した場合の処理に入る。次の鍵回復情報が存在しない時には、鍵情報を通信部12fに送り、鍵情報を回復者装置11の通信部11fに送る。なお、鍵情報を受信した場合でもなかった場合にはエラー処理とする（ステップS41）。

【0034】図5は図2の実施例における鍵回復装置13の動作のフローチャートである。鍵回復装置13が鍵回復情報ID，P（K），K（RC）を受信した場合の動作をステップS51～S61に示す。すなわち、その鍵回復情報を制御部13dを通して鍵情報取得部13aに送る。鍵回復装置13の秘密鍵Snを不図示の鍵回復装置データベース装置から得る。制御部13dを通して暗号処理を使いながら鍵回復情報の中のPn（Kn）を復号する。そして鍵情報Knを得て制御部13dに送る。制御部13dは暗号化された回復条件Kn（RC）を回復条件検証部13bに送る。回復条件検証部13bは鍵情報Knを用いてKn（RC）を復号する。回復条件検証部13bは回復条件RCとして、パスワードやIDあるいはテキストデータがある中でパスワード認識と認識する。

【0035】次にパスワード要求メッセージを作成する。パスワード要求メッセージを制御部13dを通して通信部13eに送る。通信部13eはパスワード要求メッセージを、すなわち認証要求を鍵回復情報分配装置12に送る。

【0036】次に、鍵回復装置13が受信したデータが鍵回復情報ID，P（K），K（RC）でなかった場合には、鍵回復者装置11からの認証応答メッセージかを判断する。YESの場合この動作をステップS62～S71に示す。すなわち、制御部13dはパスワード応答メッセージを回復条件検証部13bに送る。パスワード応答メッセージからパスワード①を取得する。登録されているパスワード②を取得する。パスワード①がパスワード②と等しいかを判断し、YESの場合は検証結果を制御部13dに返す。制御部13dは鍵情報メッセージ

を作成し通信部１３ｅに送る。通信部１３ｅは鍵情報メッセージを鍵回復情報分配装置１２にすなわちＫ１，Ｋ２・・・Ｋｎを鍵回復情報分配装置１２に送る。パスワード①とパスワード②が等しくない場合には、鍵回復装置１３からの認証要求に対して、回復者装置１１から送られてきた認証応答メッセージが正しくないのであるから、鍵回復装置１３は鍵情報を回復者に対して転送することができない。したがって、検証結果を制御部１３ｄにかえし、制御部１３ｄはエラーメッセージを作成し、通信部１３ｅに送る。通信部１３ｅはエラーメッセージを鍵回復情報分配装置１２に送り、このエラーメッセージは更に回復者装置１１に転送される。

【００３７】鍵回復装置が認証応答メッセージを受信した場合でもないものの時にはエラー処理として処理を終了する（ステップＳ７２）。本発明では、図２の如く、鍵回復情報に含まれている鍵回復装置１３のＩＤやアクセス先などの情報を鍵回復情報解析部１２ａ、鍵回復装置情報取得部１２ｂを使って得ることができる。

【００３８】従って、回復者装置１１は、全ての鍵回復装置１３の情報がなくても、直接通信することなく鍵回復情報分配装置１２を経由して鍵回復装置１３と通信し、データの暗号化に使った鍵を得ることができる。

【００３９】また、鍵回復情報分配装置１２の認証情報中継部１２ｃがあるので、鍵回復装置１３は、認証情報中継部１２ｃを経由して認証要求を回復者装置１１に届けることができるので、回復者を直接認証することができる。

【００４０】従って、鍵回復サービスを仲介するものがデータ鍵を不正に得ることを防げる。以下に図２に示した本発明の一実施例の全体的動作を説明する。

STEP101:回復者は、回復者装置１１の鍵回復要求部１１ａを用いて、回復する暗号文を指定する。

STEP102:暗号文は、鍵回復要求部１１ａから制御部１１ｅを通して鍵回復情報取得部１１ｇに送られる。

STEP103:鍵回復情報取得部１１ｇは、暗号文から鍵回復情報を取得する。本実施例の鍵回復情報は、栗田、宮内「公開鍵暗号を用いたファイル鍵暗号」（情報処理学会第４７回全国大会Ｐ４-197)に示されている。データ鍵Ｋを鍵回復装置の公開鍵Ｐで暗号化したＰ（Ｋ）と回復条件ＲＣをデータ鍵Ｋで暗号化したＫ（ＲＣ）を連結した鍵回復情報Ｐ（Ｋ），Ｋ（ＲＣ）①を元にして説明する（ただし、ＩＤは後述する）。なお、Ｐ（Ｋ），Ｋ（ＲＣ）で示される鍵回復情報をもとに、鍵回復装置の権限が並列に分散されている鍵回復情報として、Ｐ１（Ｋ１），Ｋ１（ＲＣ１），Ｐ２（Ｋ２），Ｋ２（ＲＣ２）・・・Ｐｎ（Ｋｎ），Ｋｎ（ＲＣｎ）②（並列方式）、鍵回復装置の権限が順序付けされている鍵回復情報として、Ｐｎ((Ｐｎ－１・・・Ｐ３（Ｐ２（Ｐ１（Ｋ），Ｋ（ＲＣ１），ＫＣ２（ＲＣ２)),ＫＣ３（ＲＣ３))・・・），ＫＣｎ（ＲＣｎ))③（順次方式）を考慮する。並列方式の鍵回復情報が，順次方式のＲＣ，Ｋｎ部分に、順次方式の鍵回復情報が、並列方式のＫｎの部分に挿入された、並列順次併用方式も考えられる。

STEP104:鍵回復情報取得部１１ｇで得られた鍵回復情報は、制御部１１ｅを通して通信部１１ｆに運ばれ、鍵回復情報分配装置１２に送られる。通信手段はＨＴＴＰプロトコルなど標準的なプロトコルを使っても良いし、鍵回復システム固有のプロトコルを用いて行われてもよい。また、鍵回復情報分配装置１２と回復者装置１１間の通信は、暗号処理部１１ｄ，１２ｄ、制御手段１１ｅ，１２ｅ、通信部１１ｆ，１２ｆによって、ＩＳＯ11770-3 Information technology-Securitytechniques-Key management Part3: Mechanisms using asymmetric techniquesに示されるような一般的な方法によって暗号化されてもよい。

STEP105:鍵回復情報分配装置１２の通信部１２ｆで受信した鍵回復情報は、制御部１２ｅに送られる。

STEP106:制御部１２ｅは、これを鍵回復情報解析部１２ａに送る。

STEP107:鍵回復情報解析部１２ａは、鍵回復情報の形態を識別し，権限分散されている場合には、それぞれの鍵回復装置１３の鍵回復情報を抽出する。②の形式の場合には、Ｐｎ（Ｋｎ），Ｋｎ（ＲＣｎ）がその情報となる。③の形式の場合には、鍵回復装置毎に情報を分けることができないので、そのまま第一の鍵回復装置にあてた鍵回復情報として扱う。

STEP108: STEP105で選ばれた鍵回復情報は、制御部１２ｅに送られ、制御部１２ｅは、鍵回復装置情報取得部１２ｂにおいて、鍵回復装置１３へのアクセス方法を得る。鍵回復装置情報取得部１２ｂは、鍵回復装置１３の情報をデータベースとしてもっても良いし、鍵回復情報のヘッダ部分から抽出してもよい。鍵回復装置１３へのアクセス先は、例えばhttp://kr.ro.jp/などのＵＲＬで示されても良いし、/C=jp/o=KR/ などのITU-TX.500で示されている識別名などで示されても良い。

STEP109:制御部１２ｅは、鍵回復情報とアクセス方法を通信部１２ｆに送り、通信部１２ｆは、アクセス方法に従って鍵回復情報を鍵回復装置１３に送る。通信手段は、ＨＴＴＰプロトコルなど標準的なプロトコルを使っても良いし、鍵回復装置固有のプロトコルを用いて行われてもよい。なお、鍵回復情報分配装置１２と鍵回復装置１３間の通信は、暗号処理部１２ｄ，１３ｃ、制御部１２ｅ，１３ｄ、通信部１２ｆ，１３ｅによって、ＩＳＯ1170-3 Information technology-Security techniques - Key management Part3: Mechanisms using asymmetric techniquesに示されるような一般的な方法によって暗号化されてもよい。

STEP110:鍵回復装置１３は、通信部１３ｅを通して鍵回復情報を受け取り、通信部１３ｅは、制御部１３ｄを通して鍵回復情報を鍵情報取得部１３ａに送る。

STEP111:鍵情報取得部１３ａは、制御部１３ｄを通して暗号処理部１３ｃを用いながら、鍵回復装置１３の秘密鍵Ｓｎを用いて、鍵回復情報Ｐｎ（Ｋｎ）を復号し、鍵情報Ｋｎを得る。この時並列方式の鍵回復情報の場合は、データ鍵Ｋを秘密化のため分散した鍵の一片が得られ、順次方式の鍵回復情報の場合には、次の鍵回復装置１３の公開鍵Ｐｎ－１でＫｎ－１とＫｎ（ＲＣ）を暗号化したものが得られる。

STEP112:鍵情報取得部１３ａで得られた鍵情報は、制御部１３ｄを通して回復条件検証部に送られる。

STEP113:回復条件検証部１３ｂは、制御部１３ｄを通して暗号処理部１３ｃを用いながら、鍵情報を用いて回復条件ＲＣを復号する。

STEP114:鍵回復条件検証部１３ｂは、復号された回復条件の種類を識別する。回復条件とは、回復者にパスワードを求め、回復者がそのパスワードを答えられれば回復者として認定するものや、回復条件がフリーテキストで書かれたものや、回復者に対する質問と答えが記述されており、質問を回復者に送り、その答えを求めるものや、一般的に知られた公開鍵方式を用いた電子署名のようなものである。本実施例では、パスワードを用いた認証が回復条件として要求されているものとする。

STEP115:回復条件検証部１３ｂは、パスワード要求メッセージを作成する。

STEP116:パスワード要求メッセージは、制御部１３ｄ，１３ｅを通して、鍵回復情報分配装置１２の通信部１２ｆに送られる。

STEP117:通信部１２ｆは、これを制御部１２ｅに送る。

STEP118:制御部１２ｅは、送られてきた情報がパスワード要求メッセージだと知ると、制御部１２ｅを通して認証情報中継部１２ｃに送る。

STEP119:認証情報中継部１２ｃは、パスワード要求メッセージを制御部１２ｅを通して通信部１２ｆに送り、通信部１２ｆは、パスワード要求メッセージを回復者装置１１の通信部１１ｆに送る。

STEP120:通信部１１ｆは、制御部１１ｅを通してパスワード要求メッセージを認証応答部１１ｂに送る。

STEP121:認証応答部１１ｂは、回復者にパスワードの入力を促す。

STEP122:回復者は、認証応答部１１ｂの要求に従いパスワードを入力する。

STEP123:認証応答部１１ｂは、回復者が入力したパスワードをもとにパスワード返答メッセージを作成する。

STEP124:認証応答部１１ｂは、パスワード返答メッセージを制御部１１ｅを通して通信部１１ｆに送る。

STEP125:通信部１１ｆは、パスワード返答メッセージを制御部１２ｅを通して認証情報中継部１２ｃに送る。

STEP126:認証情報中継部１２ｃは、制御手段１２ｅを用いてパスワード返答メッセージを通信部１２ｆに送る。

STEP127:通信部１２ｆは、パスワード返答メッセージを通信部１３ｅに送る。

STEP128:通信部１３ｅは、制御部１３ｄを通して回復条件検証部１３ｂに送る。

STEP129:回復条件検証部１３ｂは、パスワード返答メッセージ内のパスワードを検証し、その結果を制御部１３ｄに伝える。

STEP130:制御部１３ｄは、検証結果が正しければ鍵情報メッセージを、誤っていればエラーメッセージを通信部１３ｅに送る。

STEP131:通信部１３ｅは、鍵情報メッセージ、または、エラーメッセージを通信部１２ｆに送る。

STEP132:通信部１２ｆは、鍵情報メッセージ、または、エラーメッセージを制御部１２ｅに送る。

STEP133:制御部１２ｅは、エラーメッセージならそのまま通信部１２ｆ，１１ｆを用いて制御部１１ｅにエラーメッセージを送り処理を完了する。

【００４１】鍵情報メッセージであれば、次の鍵回復装置に対する鍵回復情報をSTEP105 からSTEP131 の処理を用いてその鍵回復装置に対する鍵情報を得、この処理が権限分散されている鍵回復装置の数だけ続けられる。

STEP134: STEP132の処理が終わると、制御部１２ｅは、鍵情報を通信部１２ｆを用いて通信部１１ｆに送る。

STEP135:通信部１１ｆは、制御部１１ｅを通して鍵情報を鍵回復部１１ｃに送る。

STEP136:鍵回復部１１ｃは、鍵情報をもとに鍵を回復する。並列方式の場合には、一般的な方法で秘密分散された鍵情報から鍵を回復し、順次方式の場合には、鍵情報が鍵そのものとなる。

STEP137:鍵回復部は、鍵を制御手段に送る。

STEP138:制御手段は、鍵をもとに鍵返答メッセージを作成し、通信部１２ｆを通して通信部１１ｆに送る。

STEP139:通信部１１ｆは、鍵返答メッセージを制御部１１ｅに送り、制御部１１ｅは、回復者に鍵が回復した旨を知らせて処理が完了する。

【００４２】図６は、本発明に用いられる鍵回復情報の基本フォーマットを示す。すなわち、鍵回復情報は平文（データ）をデータ鍵で暗号文とし、この暗号文に鍵回復情報を添付して回復者装置１１に記憶される。そして、鍵回復装置１３のＩＤ，鍵回復装置１３の公開鍵Ｐによってデータ鍵Ｋを暗号化し、Ｐ（Ｋ）および回復条件ＲＣを例えばパスワードとして回復条件をＫで暗号化したＫ（ＲＣ）とからなる。すなわち鍵回復情報はＩＤ，Ｐ（Ｋ），Ｋ（ＲＣ）からなり、これが暗号文に添付されている。そして、回復者がデータ鍵を暗号化した自分の公開鍵を復号化する秘密鍵を紛失した場合には、暗号文に添付されている鍵回復情報ＩＤ，Ｐ（Ｋ），Ｋ（ＲＣ）を鍵回復情報分散装置１２を介して所定の鍵回復装置ＩＤによって指定される鍵回復装置１３にアクセスする。そしてその鍵回復装置１３から鍵回復情報に含

まれた回復条件として、例えばパスワードによる認証要求が送信されると、回復者装置１１がパスワードを入力することにより鍵回復者と鍵回復装置１３との間で直接認証行為を行う。認証が成立した場合にはデータ鍵Ｋを鍵回復装置１３から鍵回復分配装置１２を介するか或いは直接回復者装置１１に転送するものである。回復者装置１１ではこのデータ鍵Ｋを用いて記憶された暗号文を回復し、平文（データ）を得る。

【００４３】図７は並列方式によって権限分散された鍵回復情報を示す図である。この場合、複数の回復者装置が存在し各々鍵回復者装置はＩＤ１，ＩＤ２，ＩＤ３，・・・ＩＤｎを有しているとする。その時に鍵ＫをＫ１，Ｋ２，Ｋ３，・・・Ｋｎにそれぞれ分割し、各鍵回復装置の公開鍵でＰ１，Ｐ２，Ｐ３，・・・Ｐｎでそれぞれの分解された鍵Ｋ１，Ｋ２，Ｋ３，・・・Ｋｎを暗号化する。そして、暗号文作成者によって定められた認証条件を示す回復条件ＲＣ１，ＲＣ２，ＲＣ３，・・・ＲＣｎをそれぞれの鍵Ｋ１，Ｋ２，Ｋ３，・・・Ｋｎで暗号化して、Ｋ１（ＲＣ１），Ｋ２（ＲＣ２），Ｋ３（ＲＣ３），・・・Ｋｎ（ＲＣｎ）を作成する。

【００４４】このようにして形成された並列方式の鍵回復情報を用いて複数の鍵回復装置に権限分散された場合に鍵回復を以下の如く行う。ＩＤ１から鍵回復装置のアクセス方法を得て、Ｐ１（Ｋ１）Ｋ１（ＲＣ１）を鍵回復装置ＩＤ１に送り秘密鍵Ｓ１でＰ１（Ｋ１）を復号し、Ｋ１でＫ１（ＲＣ１）を復号する。ＲＣ１によって、例えばパスワードを使って認証する。次に後述するようにセッション鍵Ｋｓを回復者装置１１と鍵回復装置１３との間で共有する。このセッション鍵Ｋｓを使って認証要求あるいは認証応答メッセージを暗号化して認証を行う。これによって回復者装置１１と鍵回復装置１３との直接認証を行うことができる。すなわち、鍵回復情報分配装置１２はこの認証に関与せず、従って従来例のように鍵回復情報分配装置１２が回復者になりかわって認証を行うことができず、従ってデータ鍵を得ることができない。次にＫ１をＫｓをかけて回復者装置１１に戻す。次にＩＤ２によって同様の処理を行う。そして、

外１　を得る。

【００４５】

【外１】

$$K1 \oplus K2 \cdots \oplus Kn = K$$

【００４６】図８は順次方式に従って権限分散された鍵回復情報を示し、図９は鍵回復装置１３の権限が順序付けられて作成された順次方式の鍵回復動作を示すフローチャートを示す。図８及び図９を参照して順次方式を説明する。なお図９のＫＲＩｎ－１＝図８の((Ｐｎ－１・・・Ｐ３（Ｐ２（Ｐ１（Ｋ）Ｋ（ＲＣ１），ＫＣ２（ＲＣ２））Ｋ３（ＲＣ３））・・・）ＫＣｎ（ＲＣｎ））である。ここで、ＫはＫ＝ＫＣ１のことで上述のＫではない。

【００４７】図８において、例えばＳ３でＰ３を外すとＫＲＩ２＝Ｐ２（Ｐ１（Ｋ）Ｋ（ＲＣ１），ＫＣ２（ＲＣ２）），ＫＣ３（ＲＣ３）となる。制御部がこのＫＲＩ２をＰ２（ＫＲＩ１）＝Ｐ２（Ｐ１（Ｋ）Ｋ（ＲＣ１），ＫＣ２（ＲＣ２））とＫＣ３（ＲＣ３）に分割する。Ｐ２（ＫＲＩ１）＝Ｐ２（Ｐ１（Ｋ）Ｋ（ＲＣ１），ＫＣ１（ＲＣ２）から例えばハッシュ関数をかけてＫＣ３を発生する。ＫＣ３でＲＣ３を復号する。これに従って鍵回復装置５が認証をする。認証が正しければ、次にＰ２（ＫＲＩ１）＝Ｐ２（Ｐ１（Ｋ）Ｋ（ＲＣ１），ＫＣ２（ＲＣ２））を鍵回復情報分配装置６に送る。この時はセッション鍵Ｋｓは使われない。次にＩＤ２を使ってアクセス方法を知ってＰ２（ＫＲＩ１）＝Ｐ２（Ｐ１（Ｋ）Ｋ（ＲＣ１），ＫＣ２（ＲＣ２））を鍵回復装置ＩＤ２に送る。この装置のＳ２でＰ２（Ｐ１（Ｋ）Ｋ（ＲＣ１），ＫＣ２（ＲＣ２））を復号する。Ｐ１（Ｋ）Ｋ（ＲＣ１）からハッシュを使ってＫＣ２を得る。ＫＣ２によりＫＣ２（ＲＣ２）を復号してＲＣ２を得る。ＲＣ２により認証を行って認証が成立したらＰ１（Ｋ）Ｋ（ＲＣ１）を鍵回復情報分配装置６に送り、ＩＤ１を使ってアクセス方法を知り、鍵回復装置ＩＤ１にＰ１（Ｋ）Ｋ（ＲＣ１）をＳ１によってＰ１（Ｋ）を復号しＫを得、ＫによってＫ（ＲＣ１）を復号し、ＲＣ１によって認証を行い、認証が成立したらＫを鍵回復情報分配装置を介して回復者装置に送る。この時はＫはＫｓで暗号化される。そして、各回復者装置はそれぞれのＩＤ１，ＩＤ２，ＩＤ３，・・・ＩＤｎを有し、且つそれぞれ回復条件指定ＲＣ１，ＲＣ２，ＲＣ３，・・・ＲＣｎを有する点も並列方式のフォーマットと同様である。

【００４８】なお、上記実施例では、上記鍵回復情報をもとに説明したが、他の形式の鍵回復情報の場合にも本発明の認証を回復者装置と鍵回復装置との間で直接行う方式は採用することができることは述べるまでもない。

【００４９】図１０は、鍵回復情報分配装置内に設けられたテーブルを示す。このテーブルにおいて鍵回復装置のＩＤ毎に回復装置の名前、アクセス先のアドレス、およびそのアクセスのプロトコルがレコードに記憶される。これにより、鍵回復情報から回復装置のＩＤを取得し、そのＩＤに基づいて図１０に示したテーブルを引くことにより鍵回復情報が示す所定の鍵回復装置をアクセスすることができる。ステップＳ１４０～Ｓ１４８はその動作を示す。

【００５０】図１１は認証情報中継部のフローチャートである。まず処理開始スタート後、認証時に、認証情報中継部が制御部からメッセージを受け取る。そして認証メッセージであった場合には制御部に回復者装置に認証要求メッセージを送ることを要求する。次に制御部が通信部に対して認証要求メッセージの送信指示を行い、通信部が回復者装置に認証要求メッセージを送信する。認証要求メッセージでなかった場合には認証応答メッセー

ジかを判断し、認証応答メッセージの時には制御部に回復装置に認証応答メッセージを送ることを要求する。そして、制御部が通信部に対して認証応答メッセージの送信指示をし、通信部が回復装置に認証要求メッセージを送信する。認証応答メッセージでもない場合には、エラー処理を行う。

【００５１】また、回復条件検証部１３ｂの制御フローは前述の図５で点線で示したステップパスワードの一致を見るステップのステップと同一であるので説明を省略する。

【００５２】次に、回復者装置の暗号処理部および回復者装置の暗号処理部１１ｄ，１３ｃのフローチャートを図１２，１３を参照して説明する。図１２において回復者装置の暗号処理部１１ｄは制御部１１ｃからデータが送られてきた時鍵回復情報が並列方式で構成されている場合には、Ｋ１，Ｋ２，Ｋ３，・・・Ｋｎかを判断する（ステップＳ１５１，１５２）。そして、ＹＥＳ場合には各Ｋ１～Ｋｎの排他的論理和を計算し、鍵Ｋを計算し、Ｋを制御部１１ｃに返す処理を行う（ステップＳ１５３，１５４）。もし、制御部１１ｃからのデータがＫ１，Ｋ２，Ｋ３，・・・Ｋｎでない場合には、通信のためのセッション鍵Ｋｓの共有処理動作を行い、あるいはセッション鍵Ｋｓでの復号通信処理を行う。

【００５３】図１３において、鍵回復装置１３の暗号処理部１３ｃの動作を示すと、制御部１３ｄからデータが送られてくると（ステップＳ１６１）、先ず、データがＰｎ（Ｋｎ）かを判断し、ＹＥＳであれば、鍵回復情報の鍵情報が並列方式で構成されている場合である。この時の動作はステップＳ１６１～Ｓ１６５に示す。即ち回復装置の秘密鍵Ｓｎを回復者装置のデータベースから取り出し、鍵回復装置の秘密鍵ＳｎでＰｎ（Ｋｎ）を復号し、Ｋｎを得る。そして、Ｋｎを制御部に返す。

【００５４】次に、Ｐｎ（Ｋｎ）でない場合には鍵回復情報の鍵情報が順次方式に構成されている場合である。このときの動作はステップＳ１６６～Ｓ１６９である。データがＰｎ（ＫＲＩｎ－１）かを判断する。ここで、ＫＲＩｎ－１は次の鍵回復装置の鍵回復情報のことである。その判断がＹＥＳであれば、鍵回復装置の秘密鍵Ｓｎを回復者装置のデータベースから取り出し、鍵回復装置の秘密鍵ＳｎでＰｎ（ＫＲＩｎ－１）を復号しＫＲＩｎ－１を得る。そして、ＫＲＩｎ－１を制御部１３ｄに返す。

【００５５】次に、データが順次方式による鍵回復情報の鍵情報でもない場合には、データが並列方式における回復条件であるかを判断する（ステップＳ１７０～Ｓ１７２）。すなわちデータがＫｎ，Ｋｎ（ＲＣｎ）かを判断する。その結果ＹＥＳの場合には、ＫｎでＫｎ（ＲＣｎ）を復号し、ＲＣを得、ＲＣｎを制御部に返す。さらに、データが並列方式の鍵回復条件出もない場合にはデータが順次方式の鍵回復条件であるかを判断する（ステップＳ１７３～Ｓ１７５）。すなわちデータがＫＣｎ，ＫＣｎ（ＲＣｎ）かを判断する。その結果ＹＥＳである場合には、ＫＣｎでＫＣｎ（ＲＣｎ）を復号し、ＲＣｎを得る。そして、ＲＣｎを制御部１３ａに返す。次にデータが順次方式の鍵回復条件でもない場合には、次に通信のためのセッション鍵Ｋｓの共有処理およびセッション鍵Ｋｓでの暗号通信処理に移行する。

【００５６】次に図１２、図１３を参照して回復者装置と鍵回復装置の間での通信のためのセッション鍵Ｋｓの共有化処理と、セッション鍵Ｋｓでの暗号通信処理を次に説明する。

【００５７】セッション鍵Ｋｓの共有処理は、回復者の公開鍵Ｐｒと、鍵回復装置の公開鍵Ｐｎを用いて行い、その後セッション鍵Ｋｓを使ってデータを暗号化して回復者装置と鍵回復装置との間で送受信する。暗号通信処理は、通信でのやりとりされるデータをＤＡＴＡと示し、Ｋｓで暗号、復号する対称的な処理である。

【００５８】セッション鍵Ｋｓの共有では、

１．鍵回復装置がＰｒ（Ｋｓ，Ｒ１）を作成、送信

２．回復者装置は、Ｐｒ（Ｋｓ，Ｒ１）を復号、Ｋｓ，Ｒ１′を得る

３．回復者装置がＲ１′と乱数Ｒ２を鍵回復装置のＰｎで暗号化してＰｎ（Ｒ１′，Ｒ２）を作成。Ｐｎ（Ｒ１′，Ｒ２）を送信

４．鍵回復装置がＰｎ（Ｒ１′，Ｒ２）を復号して、Ｒ１′，Ｒ２を得て、鍵回復装置が作成したＲ１と復号し得られたＲ１′を比較し、合っていれば回復者として認証され、Ｋｓを暗号通信に利用

５．鍵回復装置が４で得られたＲ２をＰｒ（Ｒ２）として暗号化、送信

６．回復者装置がＰｒ（Ｒ２）を復号して得られた情報をＲ２′として、回復者装置が発生したＲ２とＲ２′が同じであれば鍵回復装置が認証でき、Ｋｓで暗号通信を行う

という処理を示す。

【００５９】より具体的には、図１３に示す鍵回復装置１３の暗号処理のフローチャートのステップＳ１８１～Ｓ１８５において、暗号通信要求かを判断し、ＹＥＳの場合には回復者の公開鍵ＰｒをデータベースであるＤＢから取り出す。乱数を２つ発生させそれぞれセッション鍵Ｋｓ，認証子ＲＩとおく。次にＰｒ（Ｋｓ，Ｒ１）を作成し、Ｐｒ（Ｋｓ，Ｒ１）を制御部１３ｄに返す。Ｐｒ（Ｋｓ，Ｒ１）は、鍵回復装置から鍵情報分配装置を介して回復者装置に送信する。

【００６０】次に、図１２の回復者装置１１の暗号処理部１１ｄのフローチャートのステップＳ１８６～Ｓ１９１に移り、データがＰｒ（Ｋｓ，Ｒ１）かを判断し、そうである場合には、回復者の秘密鍵Ｓｒおよび鍵回復装置の公開キーＰｎをデータベースから取り出す。ＳｒでＰｒ（Ｋｓ，Ｒ１）を復号し、Ｋｓ，Ｒ１を得、Ｋｓを

メモリ保存する。乱数Ｒ２を発生し、Ｒ１′，Ｒ２を回復装置の公開鍵Ｐｎで暗号化し、Ｐｎ（Ｒ１′，Ｒ２）を作成し、Ｐｎ（Ｒ１′，Ｒ２）を制御部に返す。

【００６１】次に、図１３の鍵回復者装置１３のフローチャートのステップＳ１９４～Ｓ１９６に移り、Ｐｎ（Ｒ１′，Ｒ２）かを判断する。ＹＥＳの場合には鍵回復装置の秘密鍵Ｓｎ、回復者の公開鍵Ｐｒを鍵回復装置のＤＢから取り出す。次にＰｎ（Ｒ１／Ｒ２）をＳｎで復号し、Ｒ１′，Ｒ２を得る。次にＲ１＝Ｒ１′かを判断し、これにより回復者が正当な回復者であるかを確認する。ＹＥＳであった場合には、Ｐｒ（Ｒ２）を作成し、制御部にＫｓ，Ｐｒ（Ｒ２）を返し、Ｋｓで暗号処理指示を行ってＰｒ（Ｒ２）を回復者装置に送信する。

【００６２】次に、再度鍵情報分配装置を介して回復者装置の暗号処理フローチャートのステップＳ１９７～Ｓ２０１）に処理が移り、Ｐｒ（Ｒ２）かを判断し、ＹＥＳの場合には回復者の秘密鍵Ｓｒをデータベースから取り出し、Ｒｒ（Ｒ２）をＳｒで復号し、Ｒ２を得る。Ｒ２＝Ｒ２′かを判断しＹＥＳの場合は回復者装置が正当な回復者装置であったことが認証されて制御部にＫｓで暗号通信指示を行う。今までの処理によって回復者装置および鍵回復装置間の認証が成立し、且つ通信のためのセッション鍵Ｋｓが回復者装置および鍵回復装置において共有されたことになる。

【００６３】次に、回復者装置１１におけるデータをセッション鍵Ｋｓで暗号通信を行う過程について説明する。ここで、データとは、この例えばパスワード要求メッセージ、パスワード応答メッセージおよびデータ鍵情報Ｋ１，Ｋ２，Ｋ３，・・・Ｋｎである。

【００６４】先ず、ステップＳ２１０～Ｓ２１２′においてＫｓ（ＤＡＴＡ）かを判断し、そうである場合はＫｓをメモリから得て、ＫｓでＫｓ（ＤＡＴＡ）を復号しデータを得、そしてデータを制御部１１ｅに返す。次に、ステップＳ２１３～Ｓ２１５においてＤＡＴＡであるかを判断し、ＹＥＳの場合にはＫｓをメモリから得て、ＤＡＴＡをＫｓで暗号し、Ｋｓ（ＤＡＴＡ）を作成し、Ｋｓ（ＤＡＴＡ）を制御部１１ｅに返す。すなわち回復者装置１１の暗号処理部１１ｄにおいてＫｓ（ＤＡＴＡ）は認証要求メッセージを受信あるいは鍵情報Ｋ１，Ｋ２，Ｋ３，・・・Ｋｎを受信した場合である。また、ＤＡＴＡかは認証応答メッセージを送信する場合である。

【００６５】鍵回復装置１３においてもセッション鍵Ｋｓで暗号通信処理を行う場合の処理は図１３のフローチャートのステップＳ２１６～Ｓ２２４に示される。Ｋｓ（ＤＡＴＡ）か或いはＤＡＴＡかは回復者装置１１のＫｓ（ＤＡＴＡ）かでの暗号通信処理と同様であるから省略する。但し、鍵回復装置１３においてはＫｓ（ＤＡＴＡ）はパスワード応答メッセージを受信した場合にＹＥＳとなり、ＤＡＴＡはパスワード要求メッセージを送信する場合にＹＥＳとなる点が異なる。

【００６６】上述したように、Ｋｓ（ＤＡＴＡ）は回復者装置１１と鍵回復装置１３との間で直接転送される。鍵回復装置と回復者装置との間の認証は両者で共有されたセッションキーＫｓで暗号化されたメッセージを通信することにより行われる。一方セッションキーＫｓは鍵情報分配装置では共有されていない。鍵情報分配装置は認証に参加し、メッセージの中身をみ、あるいはメッセージを改ざんすることができない。したがって、回復者は回復者装置と鍵回復装置の間で直接認証される。

【００６７】図１４は本発明の他の実施例であり、鍵回復部２２ｄを鍵回復情報分配装置２２に設けたものである。鍵回復システム２０は、回復者装置２１、鍵回復情報分配装置２２、鍵回復装置２３からなる。

【００６８】回復者装置２１は、鍵回復要求部２１ａ、認証応答部２１ｂ、暗号処理部２１ｄ、制御部２１ｅ、通信部２１ｆからなる。鍵回復情報分配装置２２は、鍵回復情報解析部２２ａ、鍵回復装置情報取得部２２ｂ、認証情報中継装置２２ｃ、鍵回復部２１ｄ、暗号処理部２２ｅ、制御部２２ｆ、通信部２２ｇからなる。

【００６９】鍵回復装置２３は、鍵情報取得部２３ａ、回復条件検証部２３ｂ、暗号処理部２３ｃ、制御部２３ｄ、通信部２３ｅからなる。

STEP301:回復者は、回復者装置２１の鍵回復要求部２１ａを用いて、回復する暗号文を指定する。

STEP302:暗号文は、鍵回復要求部２１ａから制御部２１ｅを通して鍵回復情報取得部２１ｃに送られる。

STEP303:鍵回復情報取得部２１ｃは、暗号文から鍵回復情報を取得する。本実施例の鍵回復情報は、栗田、宮内「公開鍵暗号を用いたファイル鍵暗号」（情報処理学会第４７回全国大会Ｐ4-197)に示されている。データ鍵Ｋを鍵回復装置の公開鍵Ｐで暗号化したＰ（Ｋ）と回復条件ＲＣを鍵Ｋで暗号化したＫ（ＲＣ）を連結した鍵回復情報Ｐ（Ｋ），Ｋ（ＲＣ）①を元にして説明する（ただし、ＩＤは後述する）。なお、Ｒ（Ｋ），Ｋ（ＲＣ）で示される鍵回復情報をもとに、鍵回復装置の権限が並列に分散されている鍵回復情報として、Ｐ１（Ｋ１），Ｋ１（ＲＣ），Ｐ２（Ｋ１），Ｋ２（ＲＣ２）・・・Ｐｎ（Ｋｎ），Ｋｎ（ＲＣｎ）②（並列方式）、鍵回復装置の権限が順序付けされている鍵回復情報として、Ｐｎ((Ｐｎ－１・・・Ｐ３（Ｐ２（Ｐ１（Ｋ），Ｋ（ＲＣ１），ＫＣ２（ＲＣ２)),ＫＣ３（ＲＣ３))・・・)，ＫＣｎ（ＲＣｎ))③（順次方式）を考慮する。並列方式の鍵回復情報が、順次方式のＲＣ，Ｋｎ部分に、順次方式の鍵回復情報が、並列方式のＫｎの部分に挿入された、並列順次併用方式も考えられる。

STEP304:鍵回復情報取得部２１ｃで得られた鍵回復情報は、制御部２１ｅを通して通信部２１ｆに運ばれ、鍵回復情報分配装置２２に送られる。通信手段はＨＴＴＰプロトコルなど標準的なプロトコルを使っても良いし、鍵

回復システム固有のプロトコルを用いて行われてもよい。また、鍵回復情報分配装置２２と回復者装置２１間の通信は、暗号処理部２１ｄ，２２ｅ、制御部２１ｅ，２２ｆ、通信部２１ｆ，２２ｇによって、ＩＳＯ1170-3 Information technology-Security techniques-Key management Part3: Mechanisms using asymmetric techniquesに示されるような一般的な方法によって暗号化されてもよい。

STEP305:鍵回復情報分配装置２２の通信部２２ｇで受信した鍵回復情報は、制御部２２ｆに送られる。

STEP306:制御部２２ｆの出力は、鍵回復情報解析部２２ａに送られる。

STEP307:鍵回復情報解析部は、鍵回復情報の形態を識別し、権限分散されている場合には、それぞれの鍵回復装置２３の鍵回復情報を抽出する。❷の形式の場合には、Ｐｎ（Ｋｎ），Ｋｎ（ＲＣｎ）がその情報となる。❸の形式の場合には、鍵回復装置毎に情報を分けることができないので、そのまま第一の鍵回復装置にあてた鍵回復情報として扱う。

STEP308: STEP305で選ばれた鍵回復情報は、制御部２２ｆに送られ、制御部２２ｆは、鍵回復装置情報取得部２２ｂにおいて、鍵回復装置へのアクセス方法を得る。鍵回復装置情報取得部２２ｂは、鍵回復装置の情報をデータベースとしてもっても良いし、鍵回復情報のヘッダ部分から抽出してもよい。鍵回復装置２３へのアクセス先は、例えばhttp://kr.ro.jp/などのＵＲＬで示されても良いし、/C=jp/o=KR/ などのITU-TX.500で示されている識別名などで示されても良い。

STEP309:制御部２２ｆは、鍵回復情報とアクセス方法を通信部２２ｇに送り、通信部２２ｇは、アクセス方法に従って鍵回復情報を鍵回復装置２３に送る。通信手段は、ＨＴＴＰプロトコルなど標準的なプロトコルを使っても良いし、鍵回復装置固有のプロトコルを用いて行われてもよい。なお、鍵回復情報分配装置２２と鍵回復装置２３間の通信は、暗号処理部２２ｅ，２３ｃ、制御部２２ｆ，２３ｄ、通信部２２ｇ，２３ｅによって、ＩＳＯ1170-3 Information technology-Security techniques - Key management Part3: Mechanisms using asymmetric techniquesに示されるような一般的な方法によって暗号化されてもよい。

STEP310:鍵回復装置２３は、通信部２３ｅを通して鍵回復情報を受け取り、通信部２３ｅは、制御部２３ｄを通して鍵回復情報を鍵情報取得部２３ａに送る。

STEP311:鍵情報取得部２３ａは、制御部２３ｄを通して暗号処理部２３ｃを用いながら、鍵回復装置２３の秘密鍵Ｓｎを用いて、鍵回復情報Ｐｎ（Ｋ）を復号し、鍵情報Ｋｎを得る。この時並列方式の鍵回復情報の場合は、鍵Ｋを秘密分散した鍵の一片が得られ、順次方式の鍵回復情報の場合には、次の鍵回復装置２３に対する鍵回復情報と、その情報から生成される鍵で暗号化された回復条件が得られる。

STEP312:鍵情報取得部２３ａで得られた鍵情報は、制御部３ｂを通して回復条件検証部２３ｂに送られる。

STEP313:回復条件検証部２３ｂは、制御部２３ｄを通して暗号処理部２３ｃを用いながら、鍵情報を用いて回復条件ＲＣを復号する。

STEP314:鍵回復条件検証部２３ｂは、復号された回復条件の種類を識別する。回復条件とは、回復者にパスワードを求め、回復者がそのパスワードを答えられれば回復者として認定するものや、回復条件がフリーテキストで書かれたものや、回復者に対する質問と答えが記述されており、質問を回復者に送り、その答えを求めるものや、一般的に知られた公開鍵方式を用いた電子書名のようなものである。本実施例では、パスワードを用いた認証が回復条件として要求されているものとする。

STEP315:回復条件検証部２３ｂは、パスワード要求メッセージを作成する。

STEP316:パスワード要求メッセージは、制御部２３ｄ，通信部２３ｅを通して、鍵回復情報分配装置２２の通信部２２ｇに送られる。

STEP317:通信部２２ｇは、これを制御部２２ｆに送られる。

STEP318:鍵回復情報解析部２２ａは、送られてきた情報がパスワード要求メッセージだと知ると、制御部２２ｆを通して認証情報中継部２２ｃに送る。

STEP319:認証情報中継部２２ｃは、パスワード要求メッセージを制御手段２２ｆを通して通信部２２ｇに送り、通信部２２ｇは、パスワード要求メッセージを回復者装置２１の通信部２１ｆに送る。

STEP320:通信部２１ｆは、制御部２１ｅを通してパスワード要求メッセージを認証応答部２１ｂに送る。

STEP321:認証応答部２１ｂは、回復者にパスワードの入力を促す。

STEP322:回復者は、認証応答部２１ｂの要求に従いパスワードを入力する。

STEP323:認証応答部２１ｂは、回復者が入力したパスワードをもとにパスワード返答メッセージを作成する。

STEP324:認証応答部２１ｂは、パスワード返答メッセージを制御部２１ｆを通して通信部２１ｆに送る。

STEP325:通信部２１ｆは、パスワード返答メッセージ制御部２２ｆを通して認証情報中継部２２ｃに送る。

STEP326:認証情報中継部２２ｃは、制御手段２２ｆを用いてパスワード返答メッセージを通信部２２ｇに送る。

STEP327:通信部２２ｇは、パスワード返答メッセージを通信部２３ｅに送る。

STEP328:通信部２３ｅは、制御部２３ｄを通して回復条件検証部２３ｂに送る。

STEP329:回復条件検証部２３ｂは、パスワード返答メッセージ内のパスワードを検証し、その結果を制御部２３ｄに伝える。

STEP330:制御部２３ｄは、検証結果が正しければ鍵情報メッセージを、誤っていればエラーメッセージを通信部２３ｅに送る。
STEP331:通信部２３ｅは、鍵情報メッセージ、または、エラーメッセージを通信部２２ｇに送る。
STEP332:通信部２２ｇは、鍵情報メッセージ、または、エラーメッセージを制御部２２ｆに送る。
STEP333:制御部２２ｆは、エラーメッセージならそのまま通信部２２ｇ，２１ｆを用いて制御部２１ｅにエラーメッセージを送り処理を完了する。
STEP334:鍵情報メッセージであれば、次の鍵回復装置２３に対する鍵回復情報をSTEP305 からSTEP321 の処理を用いて処理しその鍵回復装置２３に対する鍵情報を得、この処理が権限分散されている鍵回復装置の数だけ続けられる。
STEP335: STEP332の処理が終わると、制御手段２２ｆは、鍵情報を通信部に送る。
STEP336:鍵回復部２２ｄは、鍵情報をもとに鍵を回復する。並列方式の場合には、一般的な方法で秘密分散された鍵情報から鍵を回復し、順次方式の場合には、鍵情報か鍵そのものとなる。
STEP337:鍵回復部２２ｄは、鍵を制御部２２ｆに送る。
STEP338:制御部２２ｆは、鍵をもとに鍵返答メッセージを作成し、通信部２２ｇを通して通信部２１ｆに送る。
STEP339:通信部２１ｆは、鍵返答メッセージを制御部２１ｅに送り、制御部２１ｅは、回復者に鍵が回復した旨を知らせて処理が完了する。

【００７０】図１５は、鍵回復部を回復者装置に設けた実施例において、認証動作を鍵回復情報分配装置を介さず鍵回復装置と回復者装置とを直接接続して行う実施例である。

【００７１】図１６は、鍵回復部を鍵回復情報分配装置に設けた実施例において、認証動作の際に鍵回復情報分配装置を介さず鍵回復装置と回復者装置とを直接接続して行う実施例である。

【００７２】図１７は、鍵回復部とデータ回復部を回復者装置に設けた実施例である。図１８は、鍵回復部とデータ回復部を回復者装置に設けた実施例において、認証動作を鍵回復装置と回復者装置とを直接接続して行う実施例である。

【００７３】図１９は、データ回復部と鍵回復部を鍵回復情報分配装置に設けた実施例である。図２０は、図１９の実施例において、認証動作を鍵回復装置と回復者装置とを直接接続して行う実施例である。

【００７４】図１５～図２０において、各構成要素は図１４と対応した参照符号を付し、より詳細な説明は省略する。なお、図２のように認証動作を鍵回復情報分配装置を介して行う場合は、回復者装置が鍵回復情報を鍵回復装置に送出した点で通信路が確立しているので、鍵回復装置からの認証要求は、鍵回復装置に鍵回復を要求した回復者装置との既に確立された通信路をもって行うことができる。回復者装置と鍵回復装置の認証のため通信を鍵回復情報分配装置を介さずに直接行うと、回復者装置に対して鍵回復装置が認証要求をする際の通信路を新たに確立しなければならないので、鍵回復装置が回復者装置を呼びにいった場合に回復者装置が話し中等の状態を生ずることがある。

【００７５】図２１は、本発明の鍵回復システムを実現する情報処理装置（コンピュータ）の構成図である。ＣＰＵ（中央処理装置）４３１、メモリ４３２、入力装置４３３、出力装置４３４、外部記憶装置４３５、媒体駆動装置４３６、ネットワーク接続装置４３７を備え、それらの各装置はバス４３８により互いに結合されている。

【００７６】ＣＰＵ４３１は、メモリ４３２に格納されたプログラムを実行する。メモリ４３２には、上述のプログラムの他に、処理に用いられるデータが格納されている。メモリ４３２としては、例えばＲＯＭ（read only memory）、ＲＡＭ（randomaccess memory）等が用いられる。

【００７７】入力装置４３３は入力装置１１に対応し、例えばキーボード、ポインティングデバイス等に相当する。また、出力装置４３４は出力装置４１７に対応し、表示装置やプリンタ等に相当する。

【００７８】外部記憶装置４３５は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク装置等である。この外部記憶装置４３５に、上述のプログラムとデータを保存しておき、必要に応じて、それらをメモリ４３２にロードして使用することができる。また、外部記憶装置４３５は、データベースとしても使用できる。

【００７９】媒体駆動装置４３６は、可搬記録媒体４３９を駆動し、その記憶内容にアクセスする。可搬記録媒体４３９としては、メモリカード、フロッピーディスク、ＣＤ－ＲＯＭ（compact disk read only memory）、光ディスク、光磁気ディスク等、任意のコンピュータ読み取り可能な記録媒体を使用することができる。この可搬記録媒体４３９に、上述のプログラムとデータを格納しておき、必要に応じて、それらをメモリ４３２にロードして使用することができる。

【００８０】ネットワーク接続装置４３７は、ＬＡＮ（local area network）等の任意の通信ネットワークに接続され、通信に伴うデータ変換等を行う。また、実施例は遺言書を例にとって、データ鍵Ｋを暗号化している秘密鍵を紛失し、それを鍵回復装置を用いて回復する場合について述べたが、本発明は遺言書の回復等の用途に用いられるだけではなく、通常の会社等においても使われることは勿論である。例えば会社の総務部において、秘密情報を暗号化させて保管しておいた場合に、その暗号化したデータ鍵Ｋを暗号化する公開鍵に対応する秘密鍵を紛失したり、あるいはその担当者が不在であるとき

に使用できる。さらには本発明は個人間の通信において暗号化データを通信しあう場合にも用いることができる。

【００８１】

【発明の効果】以上説明したように、本発明によれば、鍵回復情報分配装置があるため、回復装置が全ての鍵回復装置を知らなくとも権限分散した鍵回復装置にアクセスでき、且つ、回復者の認証を行うにあたって、回復者装置と鍵回復装置間の認証を直接２者間で行った上で鍵回復装置が回復者装置に鍵を返送可能となる効果を奏し、鍵回復サービスを仲介するサービスプロバイダなどの不正を防ぐことが出来、鍵回復システムにおけるセキュリティ向上に寄与するところが大きい。

【図面の簡単な説明】

【図１】本発明の原理にかかる鍵回復システムの原理を示すブロック図である。

【図２】本発明の鍵回復システムの一実施例を示すブロック図である。

【図３】図２の実施例における回復者装置の動作を示すフローチャートである。

【図４】図２の実施例における鍵回復情報分散装置の動作を示すフローチャートである。

【図５】図２の実施例における鍵回復装置の動作を示すフローチャートである。

【図６】本発明の実施例に用いられる鍵回復情報の一般的フォーマット図である。

【図７】本発明の実施例に用いられる並列方式で権限分散された鍵回復情報を示すフォーマット図である。

【図８】本発明の実施例に用いられる順次方式で権限分散された鍵回復情報のフォーマットを示す図である。

【図９】鍵回復装置の権限が順序付けられて作成された順次方式の鍵回復情報を示す順序方式のフローチャートである。

【図１０】鍵回復情報分散装置に設けられる鍵回復装置ＩＤとそのアクセス方法との対応テーブである。

【図１１】図２の鍵回復情報分散装置における認証中継部の動作を示すフローチャートである。

【図１２】図２の実施例の回復者装置における暗号処理装置処理部のフローチャートである。

【図１３】図２の実施例の鍵回復装置における暗号処理部のフローチャートである。

【図１４】本発明の他の実施例のブロック図である。

【図１５】本発明の他の実施例のブロック図である。

【図１６】本発明の他の実施例のブロック図である。

【図１７】本発明の他の実施例のブロック図である。

【図１８】本発明の他の実施例のブロック図である。

【図１９】本発明の他の実施例のブロック図である。

【図２０】本発明の他の実施例のブロック図である。

【図２１】記録媒体を有する本発明を実現するコンピュータ装置のブロック図である。

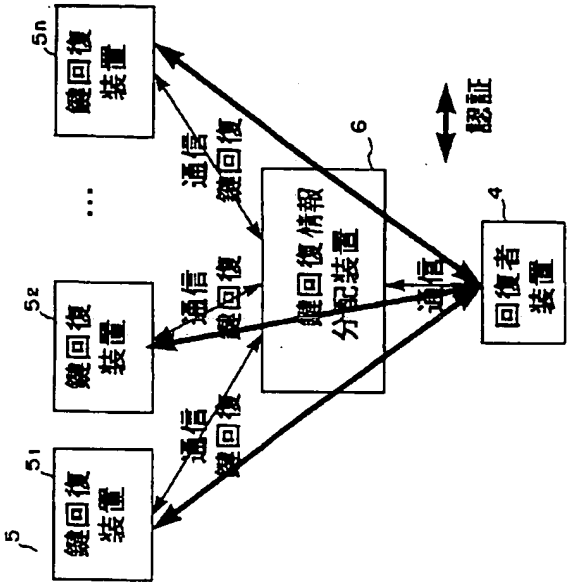
【図２２】従来例の権限を分散された鍵回復システムのブロック図である。

【符号の説明】

4　回復者装置
5　鍵回復装置
6　鍵回復情報分配装置

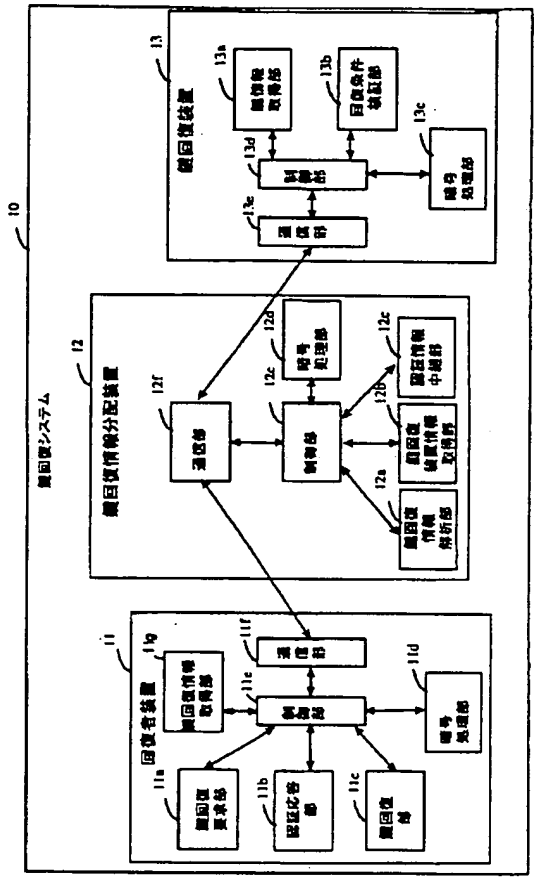
【図１】

本発明の原理にかかる
鍵回復システムの原理を示すブロック図



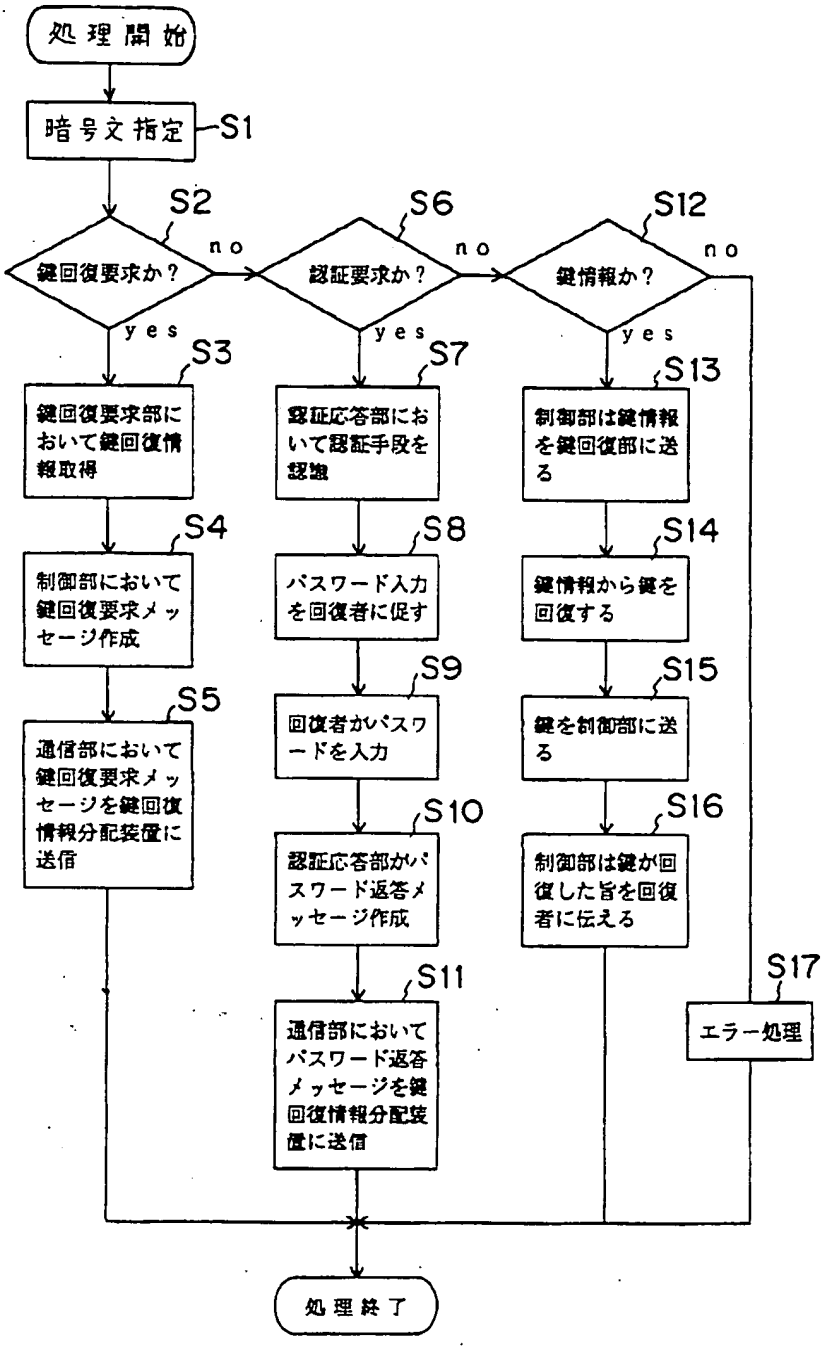
【図２】

本発明の鍵回復システムの一実施を示すブロック図



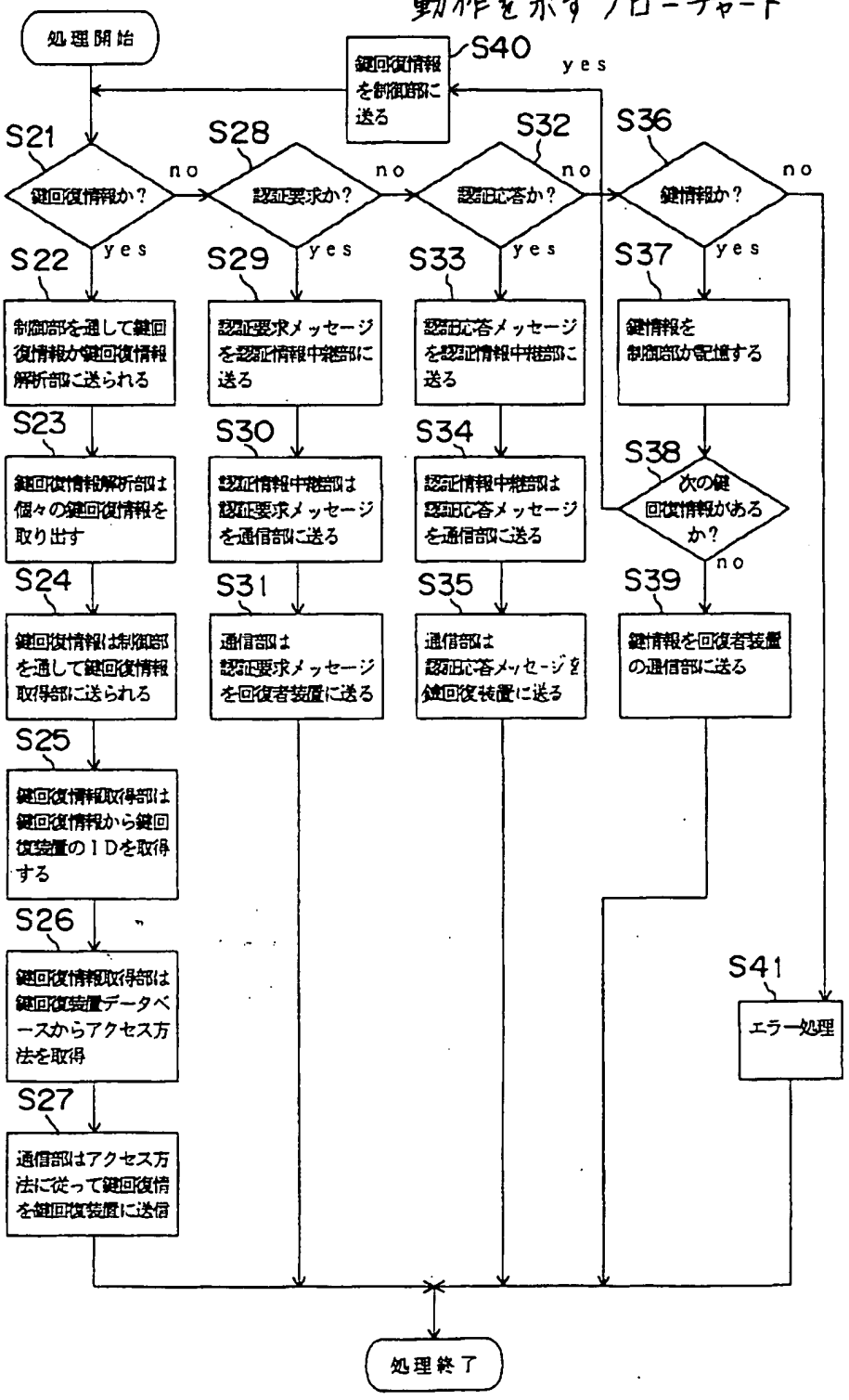
【図3】

図2の実施例における回復者装置の動作を示すフローチャート



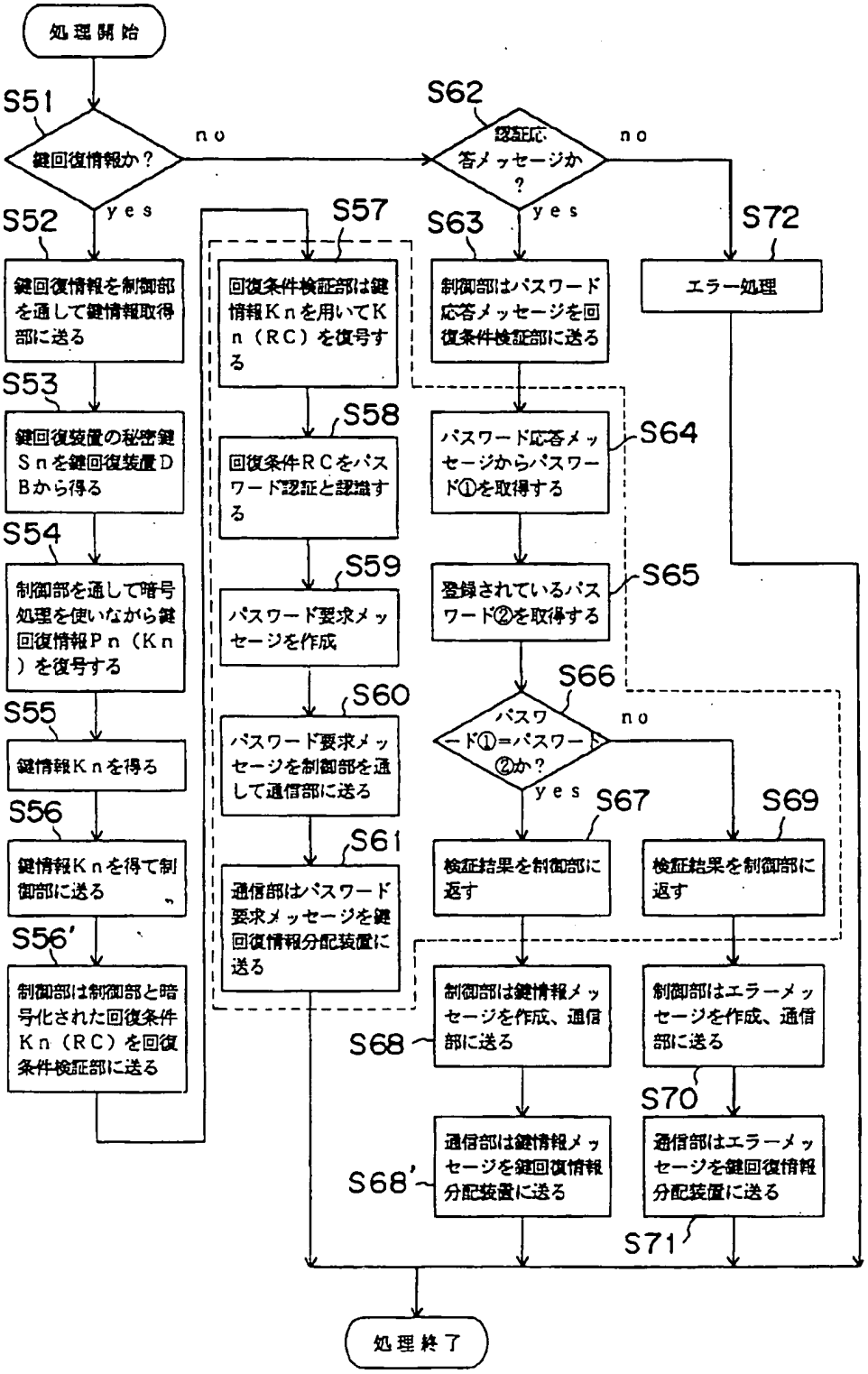
【図４】

図２の実施例における鍵回復情報分散装置の動作を示すフローチャート



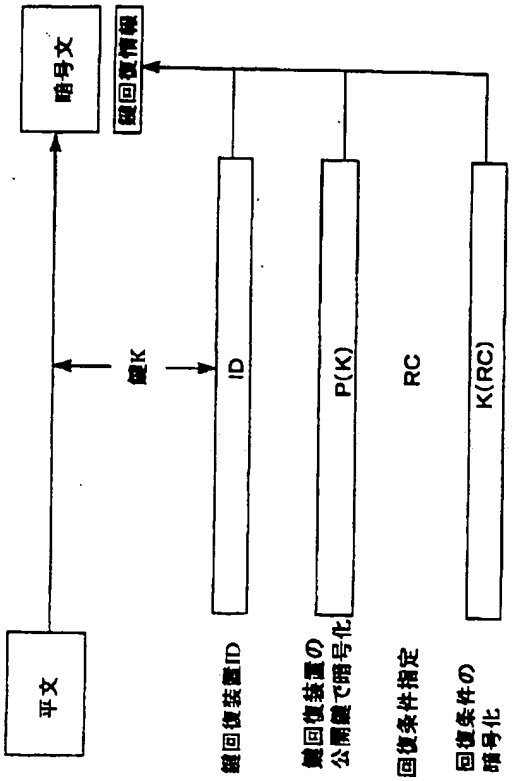
【図5】

図2の実施例における鍵回復装置の動作を示すフローチャート



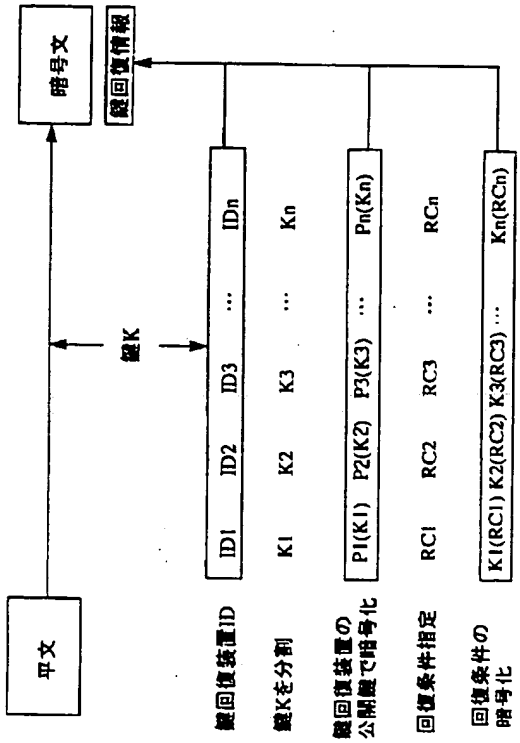
【図6】

本発明の実施例に用いられる
鍵回復情報の一般的フォーマット図



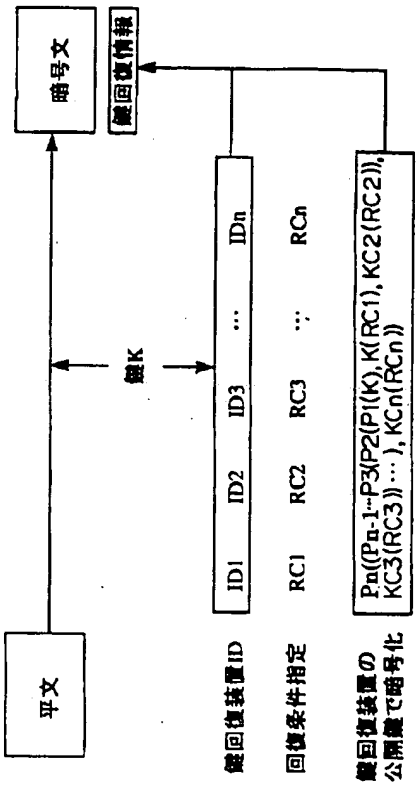
【図7】

本発明の実施例に用いられる並列方式で
権限分散された鍵回復情報を示すフォーマット図



【図8】

本発明の実施例に用いられる順次方式で
権限分散された鍵回復情報のフォーマットを示す図



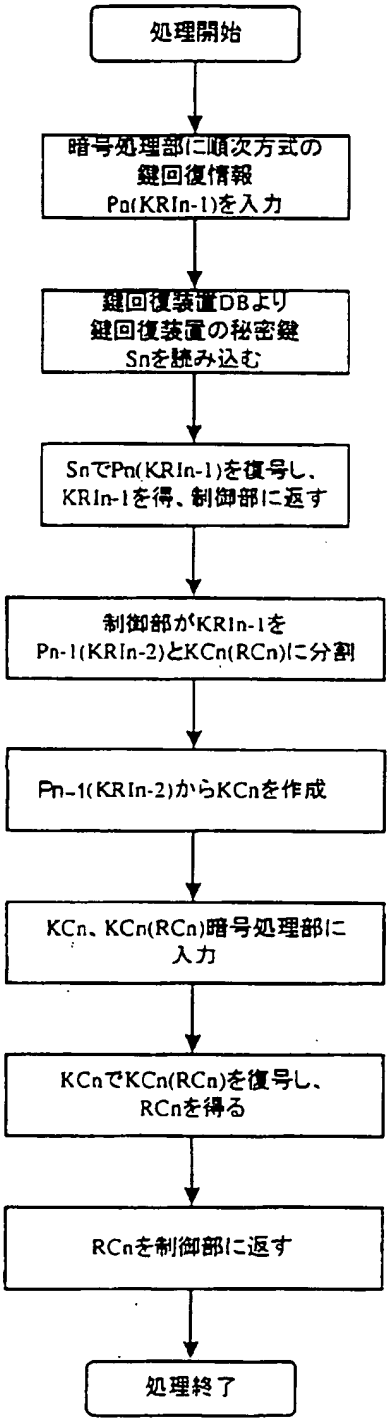
【図10】

鍵回復情報分散装置に設けられる
鍵回復装置IDとそのアクセス方法との対応テーブル

ID	名前	アクセス先	プロトコル
ID1	A社鍵回復センタ	133.160.30.7	独自プロトコル
ID2	B社鍵回復センタ	kr.or.jp	http
		…	
		…	
IDn	N回復センタ	/C=JP/o=KR/	ディレクトリサービス

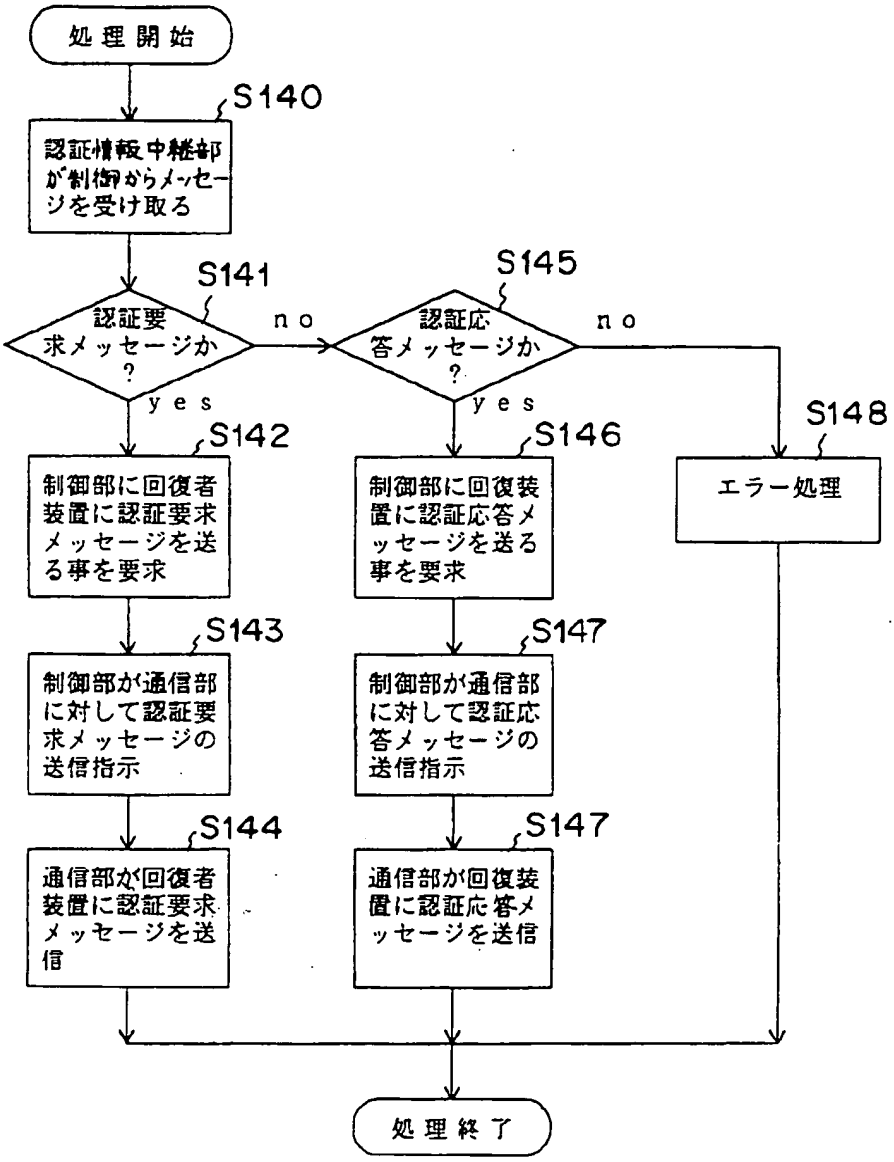
【図9】

鍵回復装置の権限が順序付けられて作成された順次方式の鍵回復動作を示すフローチャート



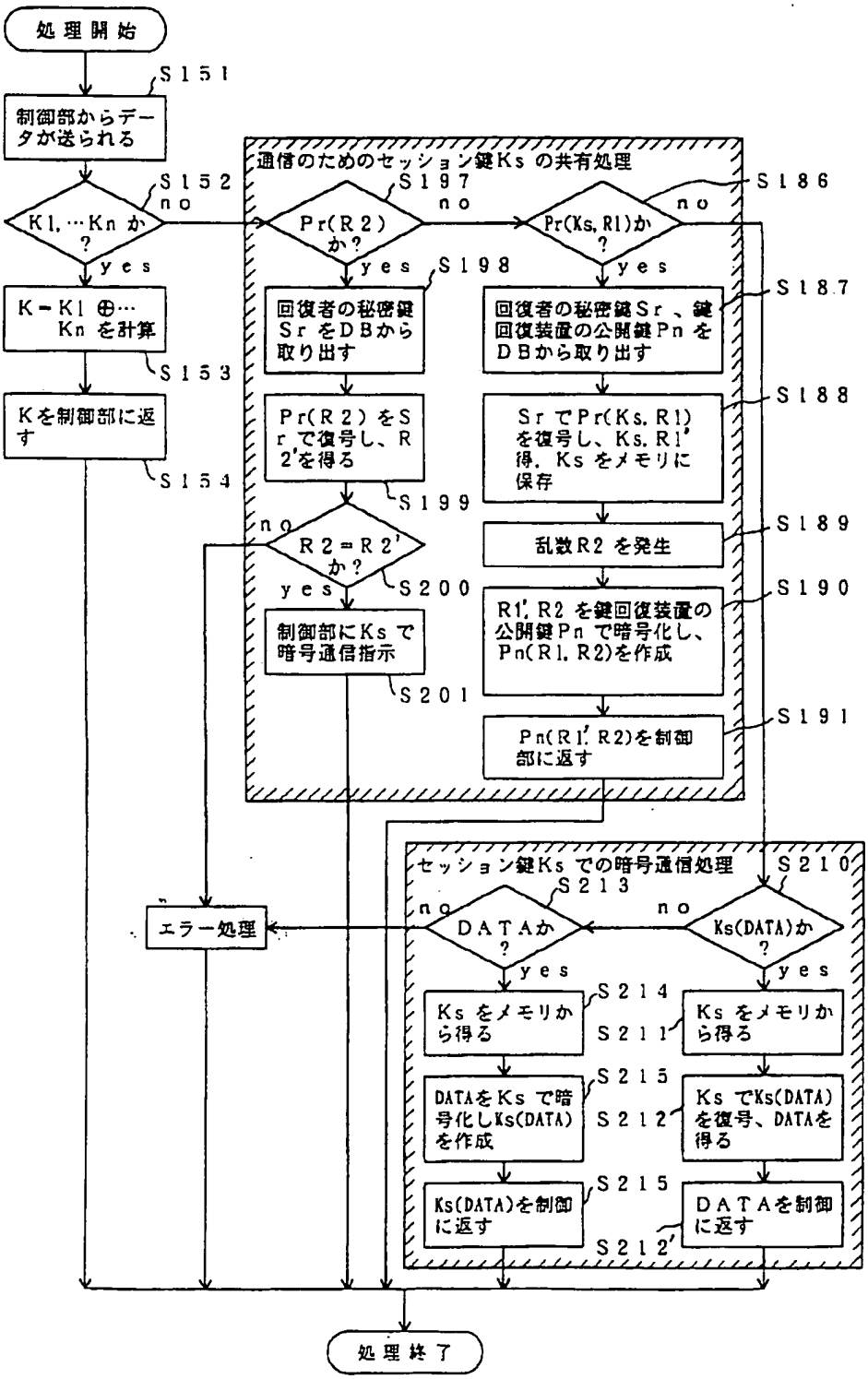
【図11】

図2の鍵回復情報分散装置における認証中継部の動作を示すフローチャート



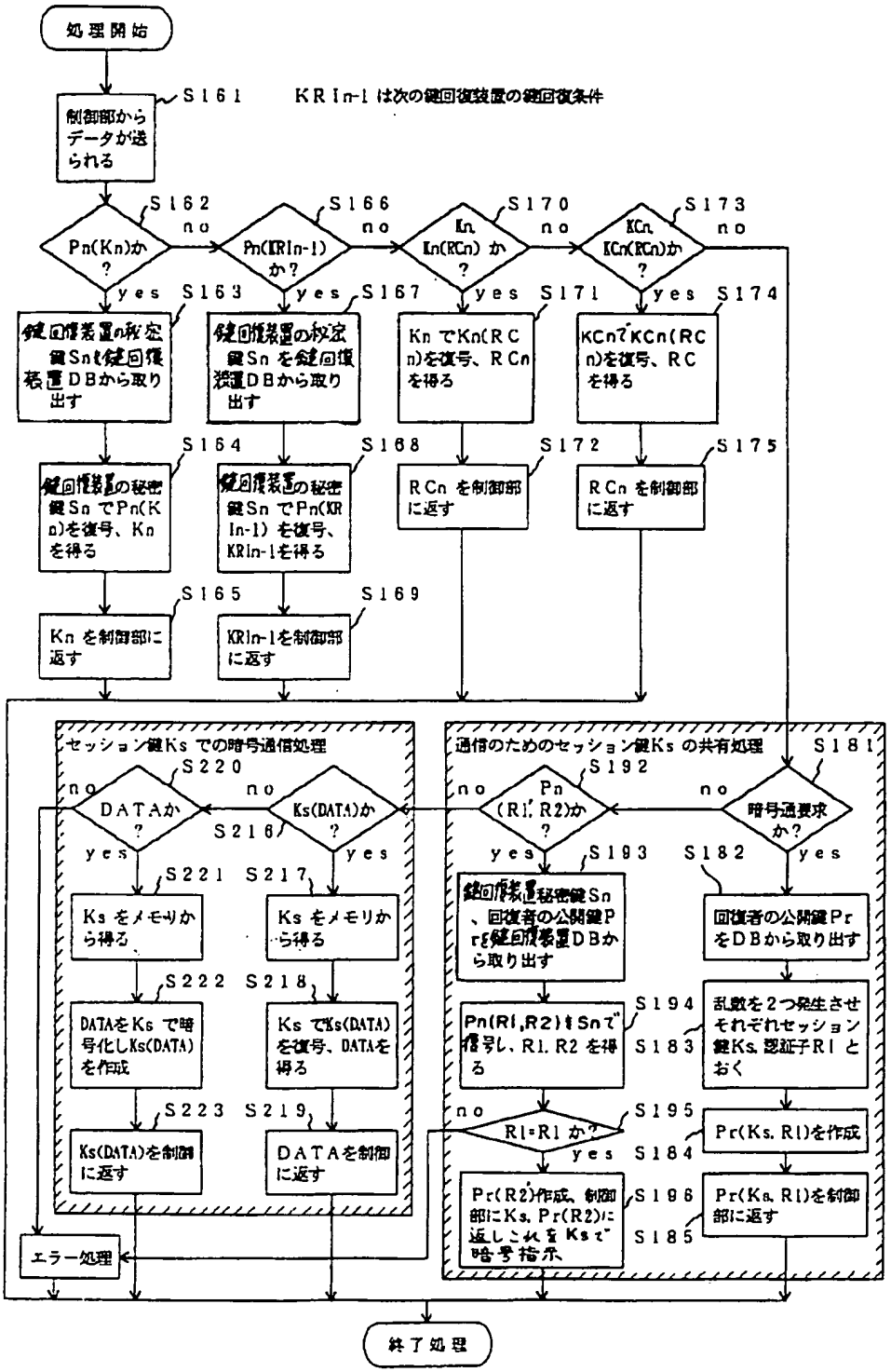
【図１２】

図２の実施例の回復者装置における暗号処理装置処理部のフローチャート



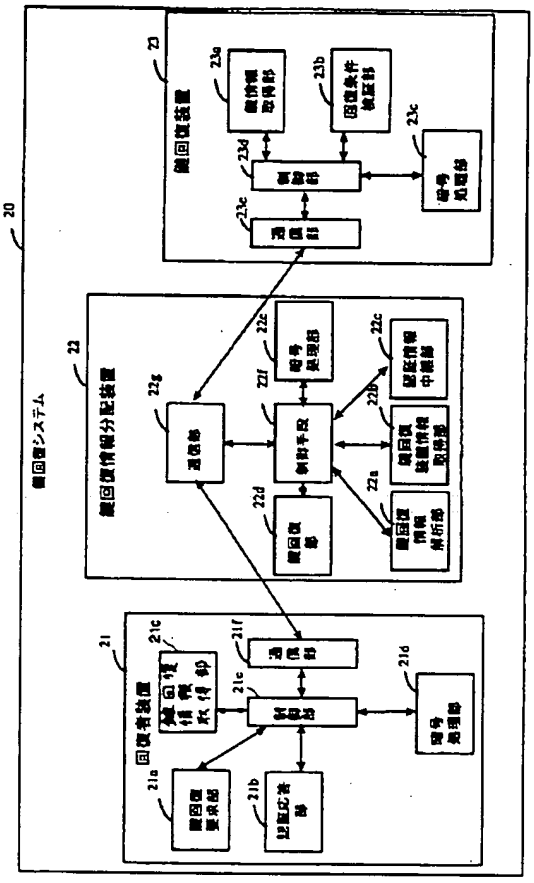
【図13】

図2の実施例の鍵回復装置における暗号処理部のフローチャート



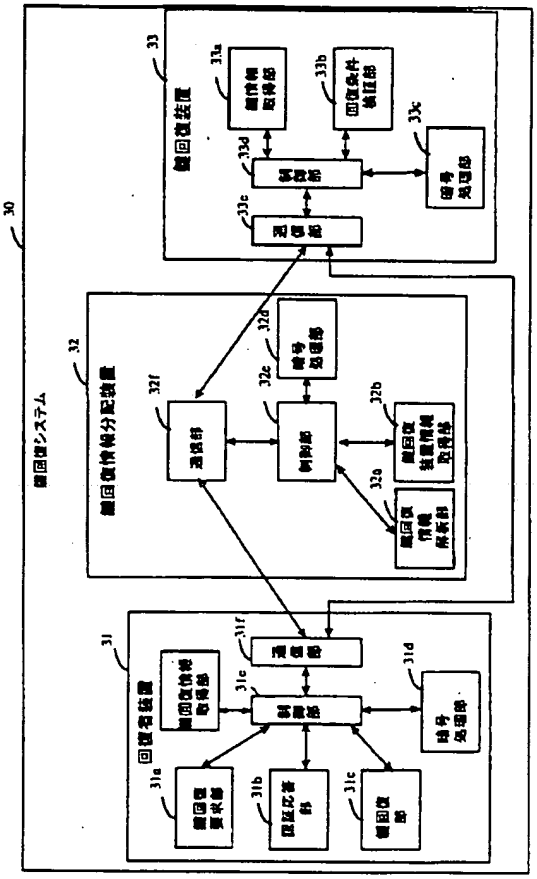
【図14】

本発明の他の実施例のブロック図



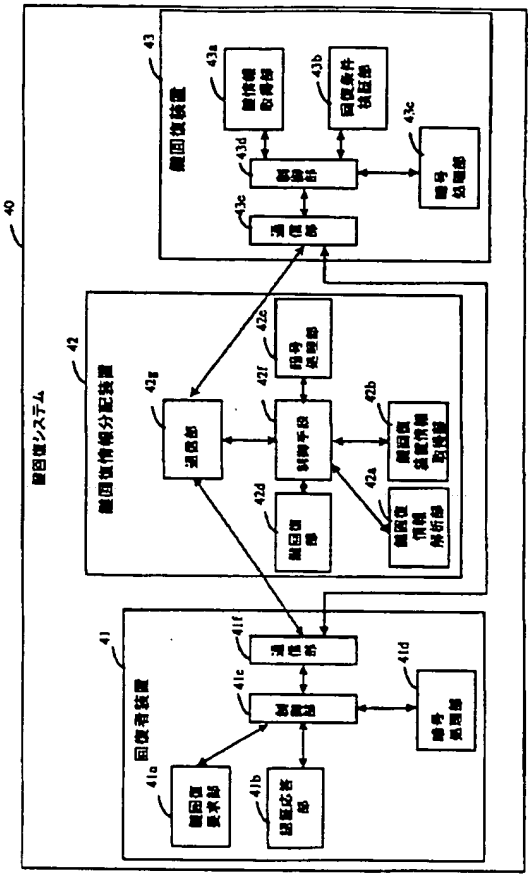
【図15】

本発明の他の実施例のブロック図



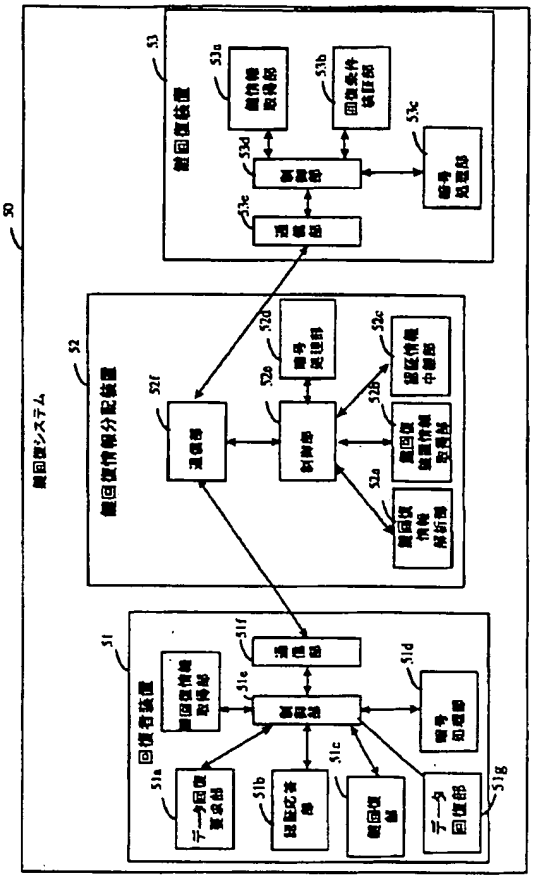
【図１６】

本発明の他の実施例のブロック図



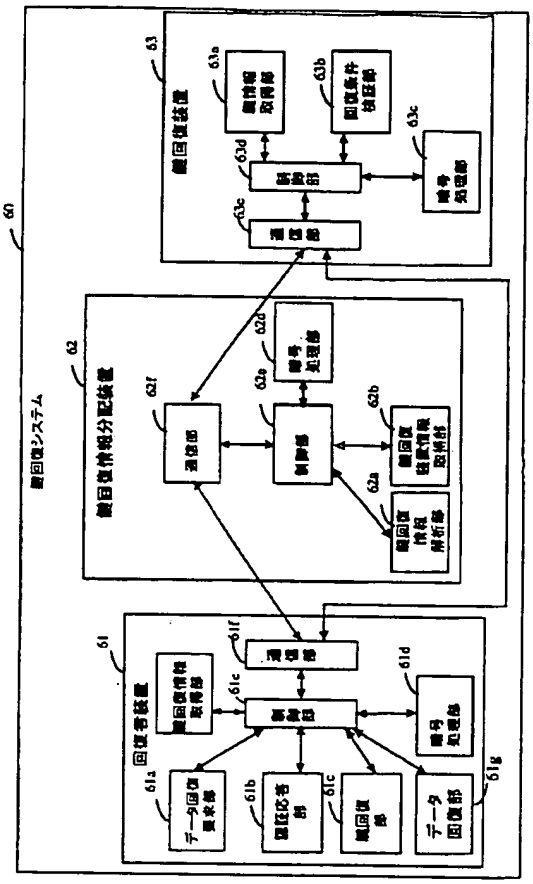
【図１７】

本発明の他の実施例のブロック図



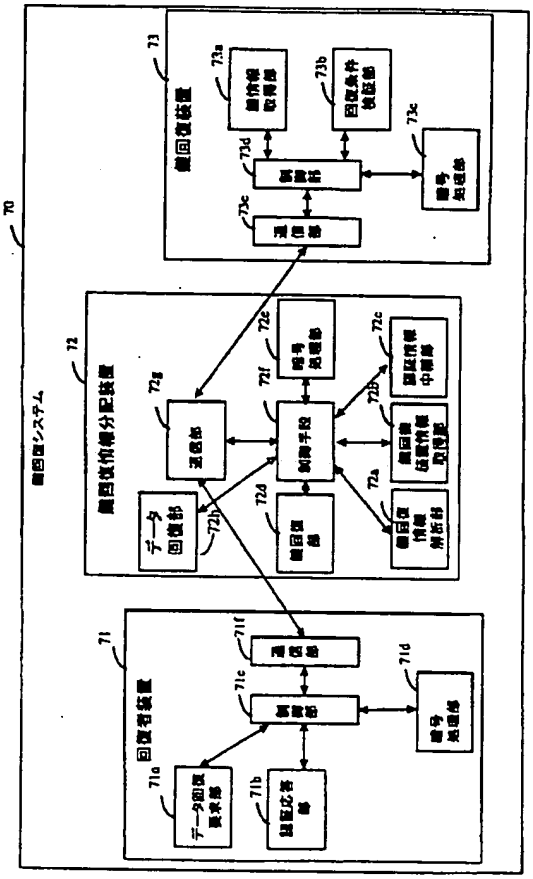
【図18】

本発明の他の実施例のブロック図



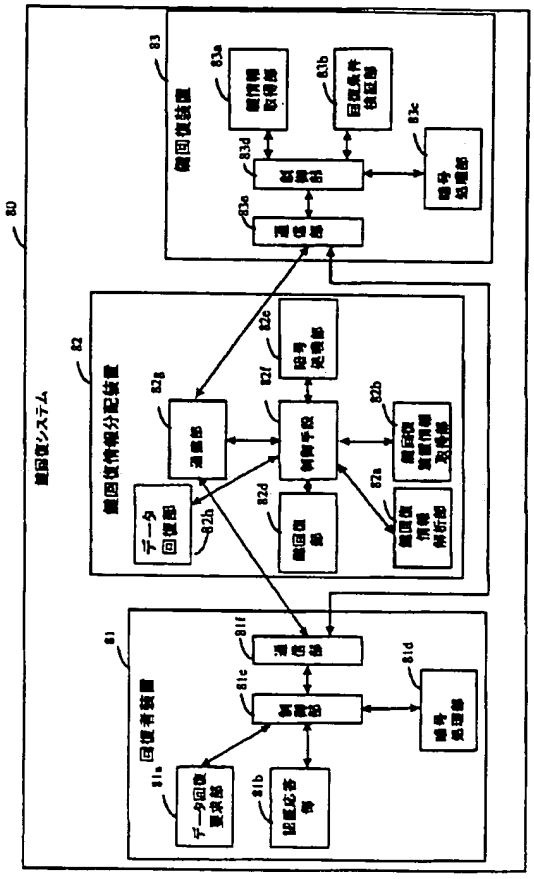
【図19】

本発明の他の実施例のブロック図



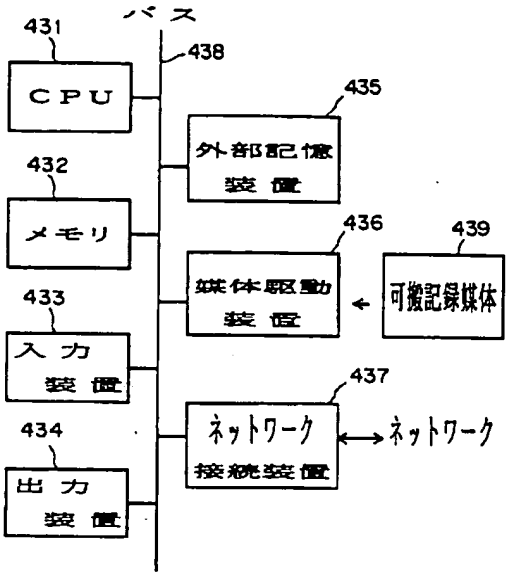
【図20】

本発明の他の実施例のブロック図



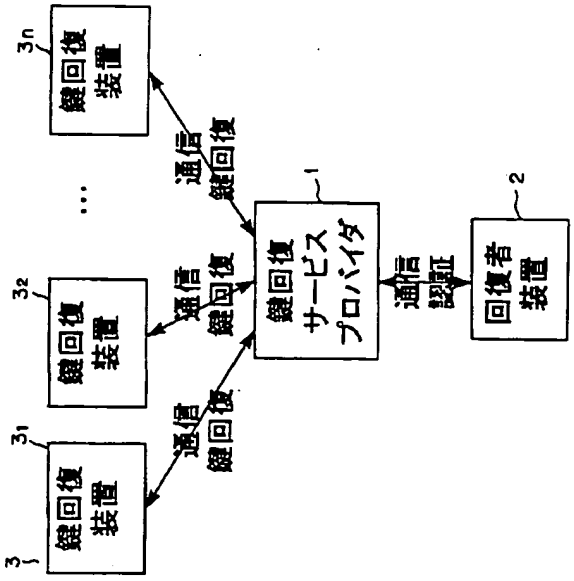
【図21】

記録媒体を有する
本発明を実現するコンピュータ装置のブロック図



【図22】

従来例の権限を分散された
鍵回復システムのブロック図



フロントページの続き

(72)発明者　安藤　宏幸
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　森田　一郎
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　黒田　康嗣
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　鳥居　直哉
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　山崎　正史
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　宮内　宏
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　佐古　和恵
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　道明　誠一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　土屋　宏嘉
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内
(72)発明者　菅野　聖子
神奈川県横浜市戸塚区戸塚町180番地　日立通信システム株式会社内